



**DoD 8320.1-M**

**Department of Defense**

---

# **DATA ADMINISTRATION PROCEDURES**

**March 1994**

**Office of the Assistant Secretary of Defense for  
Command, Control, Communications, and Intelligence**

## FOREWORD

This Manual is issued under the authority of DoD Directive 8320.1, "DoD Data Administration," September 26, 1991. It provides uniform procedures for the management and implementation of DoD Data Administration as established by DoD Directive 8320.1. This Manual supersedes DoD Instructions 5000.12 and 5000.18 and their related manuals.

This Manual applies to the Office of the Secretary of Defense (OSD), the Military Departments, the Chairman of the Joint Chiefs of Staff, the Unified Combatant Commands, the Inspector General of the Department of Defense, the Defense Agencies, and the DoD Field Activities (hereafter referred to collectively as "the DoD Components"). Its provisions are applicable to all initiatives to develop, modernize, or migrate information systems, whether automated or nonautomated.

This Manual is effective immediately; it is mandatory for use by all the DoD Components.

Send recommended changes to the Manual to:

Center for Computer Systems Engineering  
Chief, Data Standards Department  
5600 Columbia Pike  
Falls Church, VA 22041

The DoD Components may obtain copies of this Manual through their own publications channels. Approved for public release; distribution unlimited. Authorized registered users may obtain copies of this publication from:

Defense Technical Information Center (DTIC)  
8725 John J. Kingman Rd.  
Suite 0944  
Fort Belvoir, Va 22060-6218  
Commercial telephone: 1-800-225-DTIC (1-800-225-3842)  
Msorders@dgif.dtic.mil

Other Federal Agencies and the public may obtain copies from:

U.S. Department of Commerce  
National Technical Information Service (NTIS)  
5285 Port Royal Road  
Springfield, VA 22161  
Commercial telephone: 1-703-487-4650

Emmett Paige, Jr.  
(signed)

## TABLE OF CONTENTS

	<u>Page</u>
Foreword	i
Table of Contents	iii
Figures	v
References	vi
Definitions	viii
Abbreviations and Acronyms	xiii
CHAPTER 1 - INTRODUCTION	
A. Purpose	1-1
B. Applicability and Scope	1-1
C. Organization	1-3
D. Vision of DoD Data Administration	1-3
E. Strategy	1-3
F. Goals	1-4
G. Concept of Operations	1-7
CHAPTER 2 - ROLES, RELATIONSHIPS, AND RESPONSIBILITIES	
A. Introduction	2-1
B. Roles	2-1
C. Relationships	2-1
D. Responsibilities	2-3
CHAPTER 3 - PROCEDURES FOR PROGRAM ADMINISTRATION	
A. Introduction	3-1
B. Provide Policy	3-1
C. Determine Requirements	3-2
D. Provide Strategic Planning	3-5
E. Determine Resources	3-8
F. Develop Data Administration Action Plans	3-9
CHAPTER 4 - PROCEDURES FOR PROVIDING TECHNICAL INFRASTRUCTURE	
A. Introduction	4-1

B.	Establish Data Administration Procedures	4-1
C.	Establish the Defense Data Repository System (DDRS)	4-3
D.	Acquire Resources	4-4
E.	Data Model Development, Approval, and Maintenance	4-5
F.	Standard Data Development, Approval, and Maintenance	4-7
G.	Acquire Common Tools	4-9
H.	Acquire Data Collection, Distribution, and Storage Capability	4-10
I.	Develop Customer Service and Training Program	4-11

## CHAPTER 5 - PROCEDURES FOR OPERATIONAL SERVICES

A.	Introduction	5-1
B.	Manage Data Administration Action Plans	5-1
C.	Conduct Data Collection, Synchronization, and Distribution	5-3
D.	Provide Customer Service and Training	5-8
E.	Use DDRS	5-9
F.	Use DoD Data Model	5-10
G.	Use Standard, Quality Data	5-11
H.	Use Education, Training, and Consultative Services	5-12
I.	Use Common Procedures and Tools	5-13

## APPENDIXES

A.	Life-Cycle Management of Data	A-1
B.	Information Architecture	B-1
C.	Data Administration Tools	C-1
D.	Information Modeling	D-1
E.	Data Standardization	E-1
F.	Data Security and Control	F-1
G.	Database Administration Concepts	G-1

## FIGURES

<u>Figure</u>	<u>Title</u>	<u>Page</u>
1-1	Context of this Manual	1-2
1-2	Data Administration Planning Cycle	1-5
1-3	Main Data Administration Activities and Principal Products	1-8
2-1	Data Administration Authorities and Information Flows	2-2
3-1	DoD Data Administration Framework	3-3
F-1	Definitions of the goals of data integrity	F-5

## REFERENCES

- (a) Federal Information Processing Standard (FIPS) Publication (PUB) 11-3, "American National Dictionary for Information Systems," (adopted in entirety from American National Standards Institute (ANSI) X3.172-1990), February 1991
- (b) DoD Directive 8120.1, "Life-Cycle Management (LCM) of Automated Information Systems (AISs)," January 14, 1993
- (c) DoD Directive 8320.1, "DoD Data Administration," September 26, 1991
- (d) National Bureau of Standards (NBS) Special Pub 500-152, "Guide to Information Resource Dictionary System Applications: General Concepts and Strategic Systems Planning," April 1988
- (e) NBS PUB 500-149, "Guide on Data Entity Naming Conventions," October 1987
- (f) DoD 8320.1-M-1, "DoD Data Element Standardization Procedures," January 1993, authorized by DoD Directive 8320.1, September 26, 1991
- (g) DoD Directive 8000.1, "Defense Information Management (IM) Program," October 27, 1992
- (h) Assistant Secretary of Defense for Command, Control, Communication, and Intelligence Memorandum, "Interim Guidance on Functional Process Improvement," January 15, 1993
- (i) DoD Directive 5200.28, "Security Requirements for Automated Information Systems," March 21, 1988
- (j) Office of Management and Budget (OMB) Circular A-130, "Management of Federal Information Resources," January 12, 1985
- (k) "DoD Enterprise Model, Volume I: Strategic Activity and Data Models," Office of the Assistant Secretary of Defense for Command, Control, Communication, and Intelligence, January 1994
- (l) DoD Directive 5137.1, "Assistant Secretary of Defense for Command, Control, Communication, and Intelligence," February 12, 1992
- (m) DoD Directive 3405.1, "Computer Programming Language Policy," April 2, 1987
- (n) "DoD Total Quality Management Guide," February 15, 1990
- (o) Defense FAR Supplement (DFARS) 227.4, "Rights in Data and Copyrights," 1991
- (p) DoD 5025.1-M, "DoD Directives System Procedures," December 1990, authorized by DoD Directive 5025.1, December 23, 1988
- (q) DoD Instruction 7045.7, "Implementation of the Planning, Programing, and Budgeting Systems (PPBS)," May 23, 1984
- (r) FIPS PUB 184, "Integration Definition for Information Modeling (IDEF1X)," December 21, 1993
- (s) FIPS PUB 183, "Integration Definition for Function Modeling (IDEF0)," December 21, 1993
- (t) DoD Directive 5000.1, "Defense Acquisition," February 23, 1991
- (u) DoD Instruction 5000.2, "Defense Acquisition Management Policies and Procedures," February 23, 1991
- (v) DoD Directive 8120.2, "Automated Information System (AIS) Life-Cycle Management (LCM) Process, Review, and Milestone Approval Procedures," January 14, 1993

- (w) DoD Directive 8910.1, "Management and Control of Information Requirements," June 11, 1993
- (x) National Information Standards and Technology (NIST) Special Publication 500-173, "Guidelines to Data Administration," October 1989
- (y) FIPS PUB 156, "Information Resource Dictionary System (IRDS)," April 5, 1989; also "FIPS 156 Amendment," August 3, 1992 (change notice #1 to FIPS 156)



## DEFINITIONS

1. Activity. See definition 30., functional activity.
2. Activity Models. Models of the processes that make up the functional activity showing inputs, outputs, controls, and mechanisms through which the processes of the functional activity are (or will be) conducted.
3. Application Software. Software that is designed for one or more applications. (FIPS PUB 11-3, reference (a))
4. "As Is" Activity and/or Data Model. Activity and/or data model that portrays how a business process is currently structured. It is used to establish a baseline for subsequent "To Be" functional process improvement activities or programs. (See definition 41., modeling.)
5. Attribute. A property or characteristic of one or more entities; for example, COLOR, WEIGHT, SEX. Also, a property inherent in an entity or associated with that entity for database purposes (reference (a)).
6. Automated Information System (AIS). A combination of computer hardware and computer software, data, and/or telecommunications that performs functions such as collecting, processing, storing, transmitting, and displaying information. Excluded are computer resources, both hardware and software, that are: physically part of, dedicated to, or essential in real time to the mission performance of weapon systems; used for weapon system specialized training, simulation, diagnostic test and maintenance, or calibration; or used for research and development of weapon systems. (Modified from DoD Directive 8120.1, reference (b))
7. Automated Information System (AIS) Program Manager (PM). The principal official responsible for planning, directing, and managing the AIS program activities during the "Concept Exploration and Definition," "Demonstration and Validation," "Development," and "Production and Deployment" life-cycle management phases (reference (b)).
8. Conceptual Schema. Descriptive representation of data and data requirements that supports the "logical" view or data administrator's view of the data requirement. This view is represented as a semantic model of the information that is stored about objects of interest to the functional area. This view is an integrated definition of the data that is unbiased toward any single application of data and is independent of how the data is physically stored or accessed.
9. Data. A representation of facts, concepts, or instructions in a formalized manner suitable for communication, interpretation, or processing by humans or by automatic means (reference(a)).

10. Data Administration (DAdm). The responsibility for definition, organization, supervision, and protection of data within an enterprise or organization. (DoD Directive 8320.1, reference (c))
11. Data Administrator (DAd). A person or group that ensures the utility of data used within an organization by defining data policies and standards, planning for the efficient use of data, coordinating data structures among organizational components, performing logical database design, and defining data security procedures. (NBS Spec Pub 500-152, reference (d))
12. Data Architecture. The framework for organizing and defining the interrelationships of data in support of an organization's missions, functions, goals, objectives, and strategies. Data architectures provide the basis for the incremental, ordered design and development of databases based on successively more detailed levels of data modeling.
13. Data Collection. The process of obtaining information that supports a functional activity, or information requirement.
14. Data Element. A named identifier of each of the entities and their attributes that are represented in a database (reference(a)).
15. Data Entity. An object of interest to the enterprise, usually tracked by an automated system. (NBS Spec Pub 500-149, reference(e))
16. Data Integrity. In information processing, the condition in which data is accurate, current, consistent, and complete (reference(d)).
17. Data Model. In a database, the user's logical view of the data in contrast to the physically stored data, or storage structure. A description of the organization of data in a manner that reflects the information structure of an enterprise (reference (a)).
18. Data Quality. The correctness, timeliness, accuracy, completeness, relevance, and accessibility that make data appropriate for use (reference(a)).
19. Data Repository. A specialized database containing information about data, such as meaning, relationships to other data, origin, usage, and format, including the information resources needed by an organization.
20. Data Security. The protection of data from accidental or intentional modification or destruction and from accidental or intentional disclosure to unauthorized personnel (reference(a)).
21. Data Standardization. The process of documenting, reviewing, and approving unique names, definitions, characteristics and representations of data according to established procedures and conventions. (DoD 8320.1-M-1, reference (f))

22. Data Steward. The person or group that manages the development, approval, and use of data within a specified functional area, ensuring that it can be used to satisfy data requirements throughout the organization (reference(f)).
23. Data Synchronization. The timing requirements of a data element, or between and/or among data elements.
24. Data Value. A value associated with a data element. One of the allowable values of a data element. Synonym of "a data item" (reference(c)).
25. Database. A collection of interrelated data, often with controlled redundancy, organized according to a schema to serve one or more applications; the data are stored so that they can be used by different programs without concern for the data structure or organization. A common approach is used to add new data and to modify and retrieve existing data (reference (a)).
26. Database Administration (DBAdm). The activity responsible for the enforcement of the policies and standards established by the data administrator, to include providing technical support for physical database definition, design, implementation, maintenance, integrity, and security; and coordinating with computer operations technicians, system developers, vendors, and users. Database administration is oriented toward technical support for databases and the effective and efficient use of information technology resources.
27. Database Administrator (DBAd). A person or group that provides technical support for one or more databases, by defining database schemas and subschemas, by maintaining data integrity and concurrence, providing physical database design for performance optimization, and enforcing the policies, standards, and procedures set by the data administrator (reference (d)).
28. Enterprise Model. An information model(s) that presents an integrated top-level representation of processes, information flows, and data. (Derived from DoD Directive 8000.1, reference (g).)
29. External Schema. A logical description of an enterprise that may differ from the conceptual schema upon which it is based in that some entities, attributes, or relationships may be omitted, renamed, or otherwise transformed (reference (a)).
30. Functional Activity. The primary subdivision of a functional area, made up of a collection of processes that can be managed together using policies and procedures not specifically applicable to other functional activities within the functional area.
31. Functional Area. A functional area (e.g., personnel) is comprised of one or more functional activities (e.g., recruiting), each of which consists of one or more functional processes (e.g., interviews) (reference (g)).

32. Functional Process. A well-defined (or definable) set of logically related tasks and decisions within a functional activity that use resources to produce products or services.
33. Functional Process Improvement. Application of a structured methodology to define a function's "as is" and "to be" environments; current and future mission needs and end user requirements; objectives and a strategy for achieving those objectives; and a program of incremental and evolutionary improvements to processes, data, and supporting AISs that are implemented through functional, technical, and economic analysis and decision-making. (See the ASD(C3I) Memorandum, reference (h).)
34. Information. Any communication or reception of knowledge such as facts, data, or opinions, including numerical, graphic, or narrative forms, whether oral or maintained in any medium, including computerized databases, paper, microform, or magnetic tape (reference (g)).
35. Information Architecture. A framework that portrays relationships among all data and activity components identified in models. It is an abstraction based on the products of the highest level of modeling and is further refined based on the next successive levels of modeling as each area of those detailed levels are completed.
36. Internal Schema. An internal schema describes data as it is physically stored and includes all aspects of the environment in which a database is to reside (reference (a)).
37. Information System (IS). The organized collection, processing, maintenance, transmission, and dissemination of information, in accordance with defined procedures, whether automated or manual. (DoD Directive 5200.28 (reference (i)), as modified by OMB Cir A-130 (reference (j)).)
38. Logical Data Model. A model of data that represents the inherent structure of that data and is independent of individual applications of the data and also of the software or hardware mechanisms which are employed in representing and using the data.
39. Metadata. Information describing the characteristics of data; data or information about data; descriptive information about an organization's data, data activities, systems, and holdings (reference (d)).
40. Migration System. An existing AIS or a planned and approved AIS that has been officially designated to support standard processes for a functional activity applicable DoD-wide or Component-wide (reference (b)).
41. Modeling. Application of a standard, rigorous, structured methodology to create and validate a physical, mathematical, or otherwise logical representation of a system, entity, phenomenon, or process.
42. Operational Service. The activities necessary to fulfill the mission of a function or program, and to use the final products of the function or program.

43. Physical Data Model. A representation of the technologically independent information requirements in a physical environment of hardware, software, and network configurations representing them in the constraints of an existing physical environment (reference (a)).
44. Program Administration. The management activity necessary to manage a program across functional and organizational areas.
45. Repository. See definition 19., data repository.
46. Schema. A description or global model of the structure of a database (reference (a)).
47. Single Point-of-Entry. The organization(s) responsible for entering data values for a data element.
48. Standard Data Element. A data element that has been approved formally in accordance with the organization's data element standardization procedures.
49. Subject Area. A major, high-level classification of data. A group of entity types that pertains directly to a function or major topic of interest to the enterprise.
50. Technical Infrastructure. The internal framework that must be built to implement an operational service.
51. "To Be" Activity and/or Data Model. Activity and/or data models that result from a functional process improvement action or program. The "to-be" model shows how the business process will function and the data it will use after the improvement action is implemented. (See definition 41., modeling.)

## ABBREVIATIONS AND ACRONYMS

1.	AIS	Automated Information System
2.	ANSI/SPARC	American National Standards Institute's Standards Planning and Requirements Committee
3.	ASD(C3I)	Assistant Secretary of Defense for Command, Control, Communications, and Intelligence
4.	CASE	Computer Aided Software Engineering
5.	CDA	Central Design Activity
6.	CDAd	Component Data Administrator
7.	CIM	Center for Information Management
8.	DAd	Data Administrator
9.	DAdm	Data Administration
10.	DAPM	Data Administration Program Manager
11.	DAPMO	Data Administration Program Management Office
12.	DASD(IM)	Deputy Assistant Secretary of Defense for Information Management
13.	DASP	Data Administration Strategic Plan
14.	DBAd	Database Administrator
15.	DBAdm	Database Administration
16.	DBMS	Database Management System
17.	DBOF	Defense Business Operating Fund
18.	DDRS	Defense Data Repository System
19.	DISA	Defense Information Systems Agency

20. DoD	Department of Defense
21. DoD DAd	DoD Data Administrator
22. DTIC	Defense Technical Information Center
23. FAPM	Functional Activity Program Manager
24. FAd	Functional Data Administrator
25. FEA	Functional Economic Analysis
26. FIM	Functional Information Manager
27. FIPS	Federal Information Processing Standards
28. FPI	Functional Process Improvement
29. FYDP	Future Year Defense Plan
30. IDEF	Integrated Computer-Aided Manufacturing Definition
31. IM	Information Management
32. IRDS	Information Resource Dictionary System
33. IRM	Information Resource Management
34. IS	Information System
35. OSD	Office of the Secretary of Defense
36. OSD PSA	Office of the Secretary of Defense, Principal Staff Assistant
37. NBS	National Bureau of Standards
38. NIST	National Institute of Standards and Technology
39. NTIS	National Technical Information Service
40. PM	Program Manager
41. POM	Program Objective Memorandum

42. PPBS

Planning, Programming, Budgeting System



## CHAPTER 1

### INTRODUCTION

#### A. PURPOSE

1. This Manual provides uniform procedures for implementation of the policies and concepts set forth in DoD Directive 8320.1 (reference (c)) for DoD Data Administration. This Manual supports the Defense Information Management (IM) Program. Successful execution of these procedures will help to ensure that DoD data can be identified, standardized, collected, distributed, used, and disposed of with accuracy and consistency, regardless of medium or intended use as described in DoD Directive 8000.1 (reference (g)). It will also ensure the effective management of data, like other DoD resources, throughout its life-cycle. (See Appendix A.)

2. This Manual:

- a. Describes the goals of DoD Data Administration.
- b. Presents the general concept of operations for DoD Data Administration.
- c. Amplifies the data administration roles and responsibilities for DoD personnel.
- d. Provides information on data administration procedures.

Supplemental manuals provide, upon publication, detailed procedures for specific data administration activities such as data model development, approval, and maintenance; data element standardization ("DoD Data Element Standardization Procedures," reference (f)); data security; data quality assurance; and database administration. Figure 1-1 illustrates the relationship of the DoD Data Administration Directive (reference (c)), the data administration annual plan, this Manual, and its associated supplemental procedural manuals.

#### B. APPLICABILITY AND SCOPE

The applicability and scope of this Manual are identical with the Applicability and Scope statements of DoD Directive 8320.1 (reference (c)). Thus, this Manual applies to all the DoD Components; the information systems of the DoD Components; and the data elements, codes, values, and symbols in those information systems. This includes command and control systems and weapon systems. Data elements and data values that are required to be unique for use in cryptologic activities are excluded.

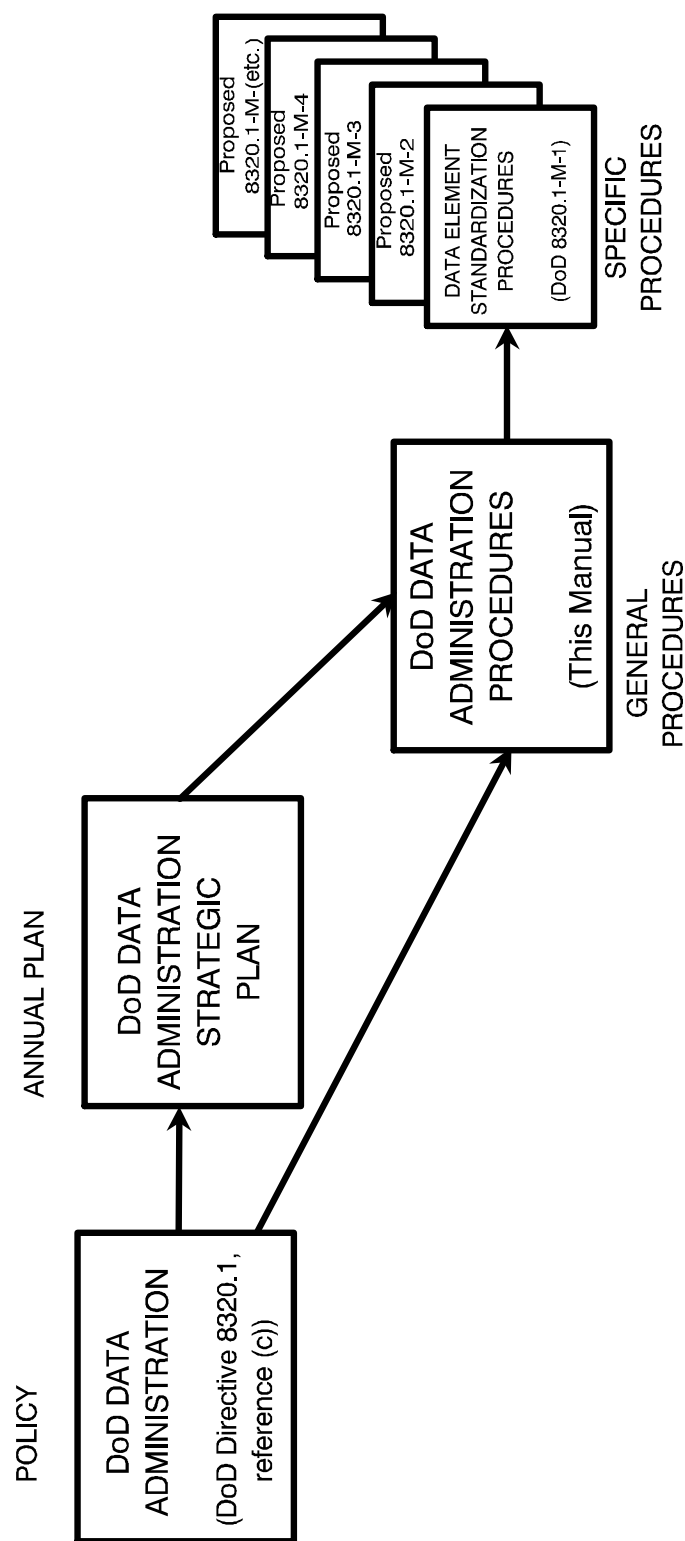


Figure 1-1 Context of this Manual



## C. ORGANIZATION

This Manual is organized into three major parts. Chapters 1 and 2 provide an introduction to data administration, including goals, the concept of operations and the roles, relationships, and responsibilities. Chapters 3 to 5 give the detailed procedures of the three main activities required in implementing a DoD Data Administration Program and using data administration products and services. The Appendices are designed either to be tutorial or to provide general information to further an understanding of data administration concepts or activities. Many of the topics in the Appendices have been, or are in the process of being, made into supplemental manuals to this Manual.

## D. VISION OF DoD DATA ADMINISTRATION

Data are valued and managed as a corporate asset that supports the Department of Defense's full range of data needs. Data are captured correctly and are available at the time needed, where needed, and for the person(s) who need it to do their job. Many disparate groups are working together to ensure and maintain interoperability and shareability of the data asset via the process described in the 8000 series of Directives. Data models and activity models are used as a principal mechanism for managing the data asset, and are aligned to each other through common missions, policies, goals, doctrines, tactics, and operations orders. Data are managed by comprehensive, effective DoD-wide data administration functions, under centralized direction, with decentralized implementation and operation. The coordinating mechanism is a centrally-managed repository that has information about data needed by the data administration community, technical development activities, and functional activities throughout the Department. Operational data are managed and stored in physical structures based on logically constructed data models and related business rules. These physical structures are implemented to maintain overall quality of the data under secure conditions in varying operational scenarios under which the Department operates. Source data are entered at their origin electronically, whenever practical, without first being hand-written or typed. Appropriate data are available to the warrior in the foxhole and the commander in headquarters, in the type and form needed for the functional process being performed.

## E. STRATEGY

1. Data administration shall be implemented in an evolutionary manner in accordance with the procedures established in this Manual. The OSD functional staff (including OSD Principal Staff Assistants (OSD PSAs)), the Chairman of the Joint Chiefs of Staff, each Functional Area and each Component respectively will establish data administration roles, relationships, and responsibilities within their function or organizational structure that correspond to those described in Chapter 2, below.

2. To promote active participation in data administration throughout the

Department, an annual DoD data administration plan, called the Data Administration Strategic Plan (DASP), shall be developed, which shall be used to define, plan, implement, and operate the DoD Data Administration Program. The DASP will contain specific objectives and activities that support accomplishment of the mission of the DoD Data Administration Program "to provide for effective, economic acquisition and use of accurate, timely, and shareable data to enhance mission performance and system interoperability."

3. Annual planning guidance is developed by the DoD Data Administrator (DoD DAd) and distributed to the Components and OSD PSAs to assist in the preparation of their data administration plans. Their data administration plans will be submitted to the DoD DAd each year. After review and consolidation, data administration plans are incorporated into a DoD DASP for approval by the DoD senior information management official, the Assistant Secretary of Defense for Command, Control, Communications, and Intelligence (ASD(C3I)). Major phases of this cycle are aligned with the DoD Program Objective Memorandum (POM) and budget cycle. Figure 1-2 graphically depicts the key phases and products of the data administration planning cycle.

## F. GOALS

The DoD Data Administration Program mission concentrates on six major goals. Each goal is a broad statement of long-term objectives for DoD Data Administration. The following goals focus on benefits necessary to realize the future vision of DoD Data Administration: (Near-, mid-, and long-term objectives for the DoD Data Administration Program in support of each goal are documented annually in the DoD DASP. The objectives are measurable and provide the means to achieve the six program goals.)

### Goal 1. Operational Central Repository

a. Goal: A centrally controlled, DoD-wide data repository is in place to receive, store, support access to, and manage standard data definitions, data formats, usage, and structures (e.g., architecture, subject area models, and other data model products). (This is the DoD Information Resource Dictionary System (IRDS) referred to in DoD Directive 8320.1, reference (c). Today, it is called the Defense Data Repository System (DDRS).)

b. Benefit: The centrally controlled, DoD repository will provide information about data needed by the data administration community, technical development activities, and functional activities throughout the Department (e.g., data element definitions, data format, and data usage). The repository will provide the information necessary to manage and store data in physical structures that are based on logically constructed data models and related business rules. This will significantly improve the accessing, sharing, and reconciling of information.

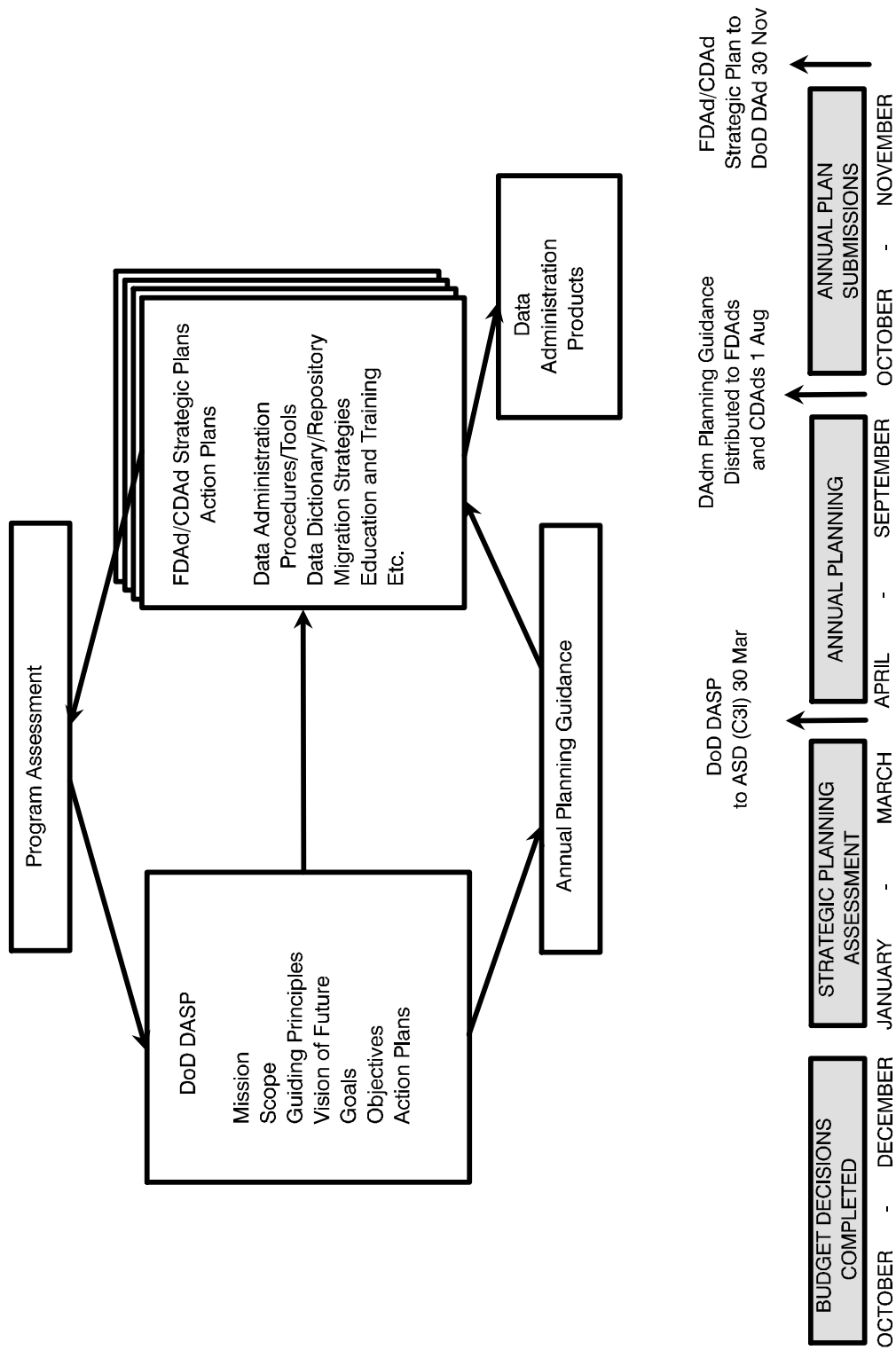


Figure 1-2 Data Administration Planning Cycle



## Goal 2. Standard Data

a. Goal: Standard data elements, data models, and data architectures exist and facilitate data sharing, data quality, reuse, single point-of-entry, and the integration of DoD databases. (As stated in DoD Directive 8320.1, reference (c), applicable federal, national, and international standards will be used before DoD standards are created.)

b. Benefit: Data standards will be implemented across the Department. Standardizing data descriptions and attributes for data will be simplified as a result of applying a data modeling methodology. It will provide a common vocabulary for the Department to use in exchanging and sharing information. It will support integrated operations among Functional Areas and facilitate good decision-making. Standard data will promote integrated operations between the Department of Defense and its suppliers, and among DoD Components. Standard data will increase interoperability among operational forces and among DoD Functional Areas in support of military operations. It will also facilitate management and control of data duplication and/or redundancy, contribute to minimizing data processing and storage costs, and improve data integrity. Standard data will be used, not only in automated information systems, but also, in manual information systems, forms, publications, reports, records and messages.

## Goal 3. Use of Common Procedures and Tools

a. Goal: Common procedures and automated tools are used and continually improved to support functional managers, data administrators, and the technical support community in providing, maintaining, and using standard data products.

b. Benefit: Architectural standards and data management and data handling procedures will guide the information system design process, and automated tools will support the reuse of data and software. Data administration products and services will be used extensively to meet the requirements of new automated information system development methods and will result in reduced development cost and time.

## Goal 4. Quality Data

a. Goal: A data quality assurance and data security program ensures that DoD operations and decision-making are supported with data meeting needs of availability, accuracy, timeliness, integrity, and need-to-know requirements.

b. Benefit: DoD personnel will use quality data for planning and analysis; as a result, decision-making will be improved. Transactions and the exchange of technical and management information will be handled more quickly and accurately. In



turn, a cost-effective operation and low overhead will be maintained.

Goal 5. Education, Training, and Consultation Services

a. Goal: Data administration training, education, consultation services, and materials designed to support data administration goals are available to and used by a broad spectrum of practitioners within the Department of Defense and the DoD support community.

b. Benefit: Data administration education and training programs for functional managers, data administrators, and the DoD support community will improve understanding, communication, and the acceptance of new roles and responsibilities. Consultation services will provide expert technical assistance.

Goal 6. Effective Infrastructure

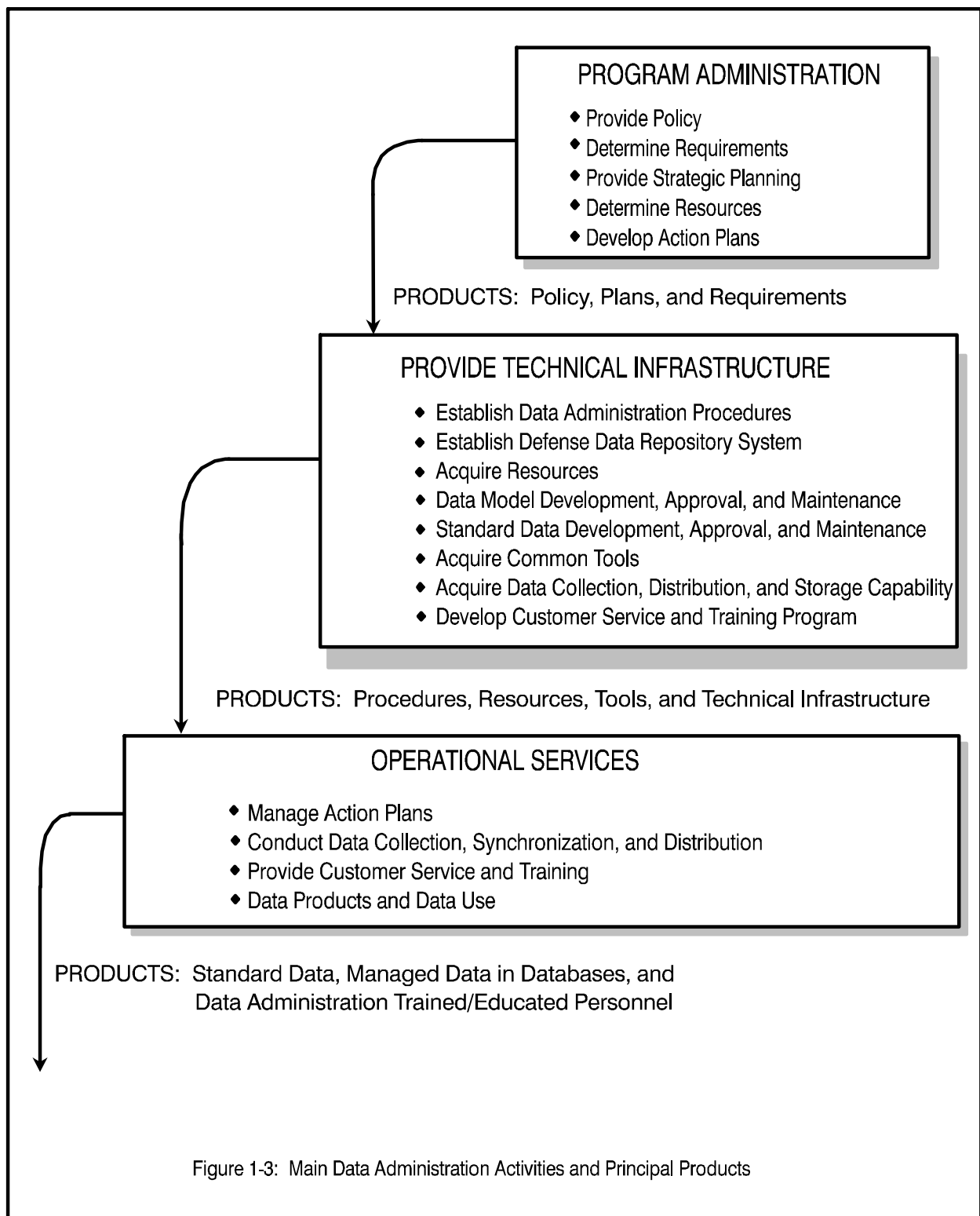
a. Goal: Data administration organizations are in place throughout the Department of Defense, are supported by senior management, serve functional managers, are staffed and prepared to assist the technical development activities, and provide the interfaces and leadership essential to improved data management.

b. Benefit: Data administration will be established throughout the Department of Defense and recognized as a cornerstone of Defense IM. Functional managers, data administrators, technical development activities, and functional activities will accept specific responsibilities for managing data. This will support the acquisition, distribution, and use of effective, efficient data resources and services.

G. CONCEPT OF OPERATIONS

1. The DoD Data Administration Program goals concentrate on targets necessary to accomplish the DoD Data Administration Program mission. The data products (and services) made available by the Program can then be used by functional activities and technical development activities (see Chapter 2 , section C., below.) to do their jobs through comprehensive and cost-effective data administration operations. The final products of the program (e.g., standard data, managed data in databases) are then made available to personnel at all levels of the Department of Defense.

2. A set of products is associated with each of the main functional activities of the DoD Data Administration Program: Program Administration, Provide Technical Infrastructure, and Operational Services. These activities relate directly to the DoD Activity Model that is part of the DoD Enterprise Model (reference (k)). There are a set of activities that describe the development of the products for each main activity. Figure 1-3, below, shows the main activities and the principal products of each one.



3. The DoD Data Administration Program is implemented with three primary roles at: departmental, functional, and Component level. (See DoD Directive 8320.1, reference (c).) The entire data administration community must work together to make the DoD Data Administration Program products available. The following is a brief discussion of the parts that each level and role contribute to DoD Data Administration: (Chapter 2, section D., below, gives more detail about the data administration responsibilities.)

a. Departmental. The DoD Data Administration Program is implemented at the departmental level under the supervision of the DoD DAd as the designated representative of the Department's senior information management official. The Defense Information Systems Agency (DISA), which has established a Data Administration Program Management Office (DAPMO) to support the DoD DAd. The DoD DAd receives policy guidance from the ASD(C3I) or the Deputy Assistant Secretary of Defense for Information Management (DASD(IM)) acting on the assistant secretary's behalf. The DoD DAd responsibilities include: development and implementation of DAdm policy, guidelines, and procedures; development and maintenance of the DDRS and the DoD Data Model; technical review of logical data models prepared by Functional Areas, Components, or others, upon request; technical review of DoD candidate standard data elements; development of the DoD DASP; and development of DAdm training, education classes, and material.

b. Functional. The Functional Data Administrator (FAd) are designated by an OSD PSA to implement the DoD Data Administration Program within the Functional Area. FAdS define the data requirements for their Functional Area by coordinating with functional experts and, particularly, with the Functional Activity Program Managers (FAPMs) who also are designated by an OSD PSA. FAdS are the data stewards for data belonging to their Functional Area. Often the stewardship of a data requirement resides in a Functional Area different from the Functional Area in which the data requirement was first identified. In such cases, the FAd of the Functional Area in which the data requirement resides becomes the data steward. For example, the requirement for a unique identifier for person may be identified in the Finance Area but, logically, the data steward is the Personnel Area. The data steward is responsible for conducting the functional review of data when it is submitted as DoD candidate standard data, and will ensure the applicability of the standard data across the Department. The data steward also is responsible for identification of the definitive source(s) for the data values of resulting standard data elements. These values are what is actually stored in databases throughout the Department. FAdS also prepare annual data administration plans that will be incorporated into the annual DoD DASP. They maintain data models of their functional view of the DoD Data Model (See Appendix B.) and ensure that technical development activities that support the functional area comply with DoD Data Administration policies and procedures.

c. Component. The Component Data Administrator (CAd) implements the DoD Data Administration Program within the Component. They assist in the

identification, definition, and organization of the data requirements for all functional areas in their organization. CDAds act as a liaison and assist in adjudicating data administration conflicts within the Component, facilitating inter- and intra-Component coordination along functional lines, and supporting and encouraging working groups to address data administration issues. They are responsible for the Component's functional review of DoD candidate data elements and for identifying any cross-functional impact on the Component. CDAds should assist FDAds in identifying and accessing functional experts within the Component and facilitate appropriate data source designation for the single point-of-entry for DoD standard data element values. Components may be designated by the steward FDAd as the definitive source for the data values of the resulting data elements. CDAds prepare strategic plans that will be incorporated into the annual DoD DASP, maintain models of their Component view of the DoD Data Model (see Appendix B), and ensure that technical development activities that support the Component comply with DoD Data Administration policies and procedures.

## CHAPTER 2

### ROLES, RELATIONSHIPS, AND RESPONSIBILITIES

#### A. INTRODUCTION

The data administration community has many members each with specific roles and interlocking relationships with other members of the community. Members also have relationships outside the data administration community whose support is essential to the success of DoD Data Administration. This Chapter identifies the key roles and responsibilities within the data administration community and the critical relationships with activities outside the data administration community.

#### B. ROLES

1. DoD Directive 8320.1 (reference (c)) identifies three primary data administration roles: DoD Data Administrator (DoD DAd), Functional Data Administrator (FDAd), and Component Data Administrator (CDAd). The ASD(C3I) Memorandum (reference (h)) identifies the Functional Activity Program Manager (FAPM) and the Technical Development Activities with whom the data administration community must interact. Figure 2-1, below, shows these roles and the principal information flows within the context of the DoD Data Administration Program.

2. The principal official responsible for directing activities during concept exploration, definition, demonstration, validation, development, production, and deployment life-cycle management phases of an information system is the Automated Information System (AIS) Program Manager (PM). Regardless of their title, the official designated to ensure an information system is put into operation has specific relationships and responsibilities with respect to data administration. Subsequent use of the term AIS PM in this document refers to all such officials, even if the information system is not automated and/or is not considered to be "major."

3. The relationships among the data administration roles are discussed in greater detail in section C. of this Chapter, below. Responsibilities associated with the data administration roles are defined in DoD Directive 8320.1 (reference (c)). More explicit responsibilities are identified in section D. of this Chapter, below.

#### C. RELATIONSHIPS

Data administration relationships exist among personnel in three broad areas:

1. Data Administration Area. The ASD(C3I), as the designated senior DoD

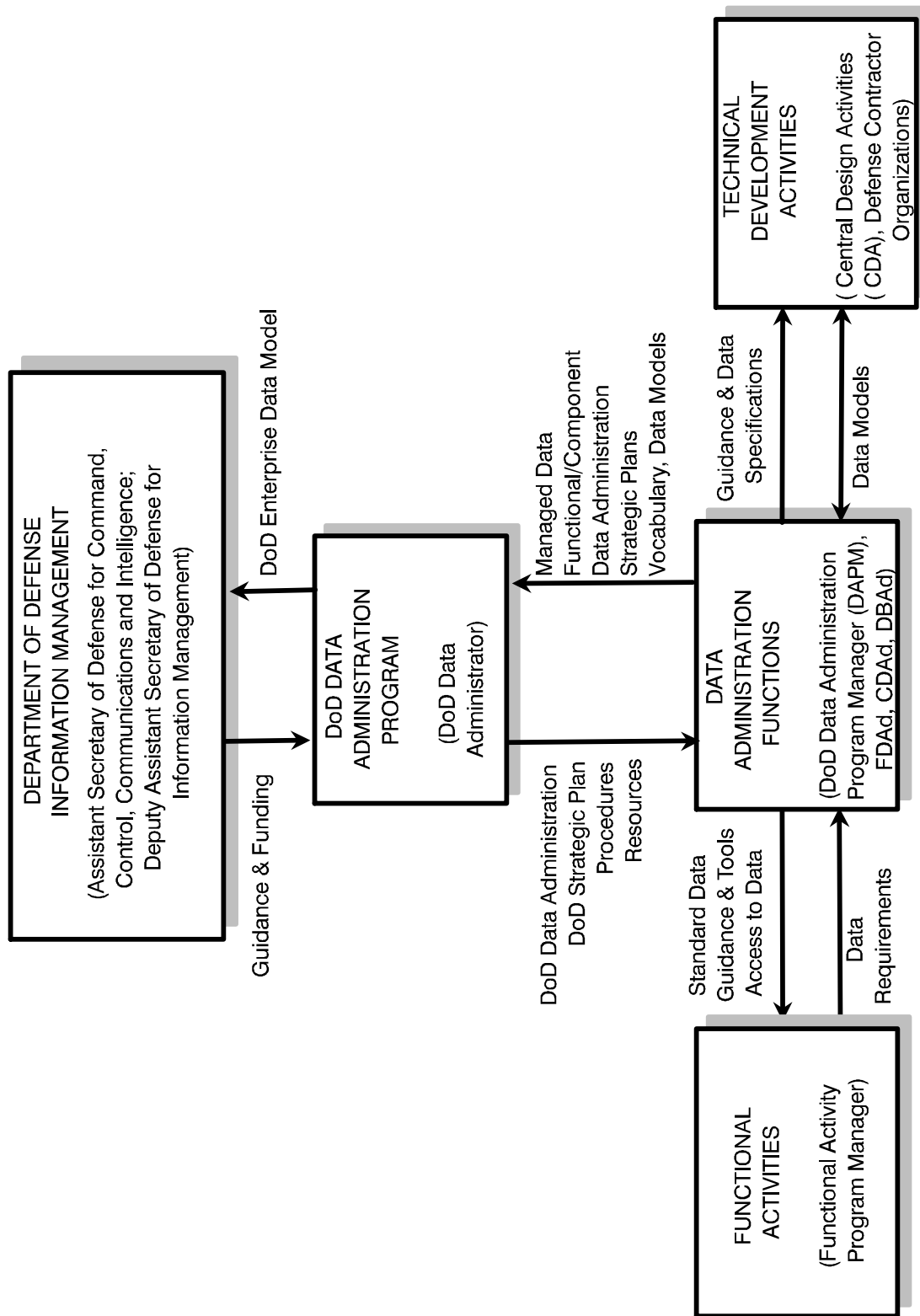


FIGURE 2-1 Data Administration Authorities and Information Flows

information management official (DoD Directive 5137.1, reference (I)), also is responsible for DoD Data Administration. The DASD(IM) acts on the ASD(C3I)'s behalf to oversee the DoD Data Administration Program. The DoD DAd is responsible for the overall management and execution of the DoD Data Administration Program and for ensuring the technical correctness and consistency of data administration products as well as developing data administration procedures, handbooks, and training materials. FDAdS and CDAdS are responsible for managing and implementing data administration within their DoD Functional Area or Component, respectively. While CDAdS and FDAdS need to have data administration expertise, it is essential that they be familiar with their Component or Functional Area. The data administration community is responsible for managing data products and making them available to both functional activities and technical development activities. The specific data products are: standard data elements and their characteristics, data models, data specifications, and actual data values.

2. Functional Activities. Each major mission area of the Department of Defense is made up of one or more Functional Areas, and each Functional Area is made up of one or more functional activities. The OSD PSAs may choose to make a single FAPM responsible for all functional activities within the functional area, or may identify a separate FAPM for each functional activity. FDAdS are responsible for Functional Areas of information at the Department (i.e., Office of the Secretary of Defense) level (e.g., Health Affairs or Acquisition) and must work closely with the FAPM to identify and define functional data requirements. Corresponding positions should exist within the Components, and in subordinate organizations within the Component, to identify and define functional activities and data requirements respectively. DASD(IM) Functional Information Managers DASD(IM) FIMs are on the OSD staff and facilitate work in, and among, the Functional Areas. AIS PMs must work closely with database administrators and technical development activities to ensure that the data in their ISs are effectively and efficiently managed.

3. Technical Development Activities. These organizations are responsible for developing application software programs, and providing information systems and services to DoD functional activities through information system design, development, and maintenance. They are responsible for developing logical data models for the information system and provide database design specifications. Technical development activities must work with data administrators to meet the data requirements of the Functional Areas, either by using existing standard data elements and specifications, or by helping develop new ones. The relationships are depicted in Figure 2-1, above, within the context of the DoD Data Administration Program. Technical development activities may be DoD organizations, known as Central Design Activities; contractors; or other government agencies.

#### D. RESPONSIBILITIES

1. Data administration responsibilities are divided among the main activities:

Program Administration, Provide Technical Infrastructure, and Operational Services. These relate directly to the DoD Enterprise Model (reference (k)). The responsibilities are distributed among the three main activities.

2. The data administration responsibilities designated for each of the roles are interrelated through the various levels of reporting authority, and the functional relationships and products produced and used.

3. DoD organizations responsible for implementing the procedures in this Manual must assign the responsibilities identified in this Chapter to specific positions within the organization. Each organization will identify the office(s) and/or position(s) responsible for each procedural action so that the organization can quickly contact them to address relevant data administration matters.

4. Responsibilities directly associated with DoD Data Administration are distributed among the primary roles cited in section B. of this Chapter, above, but some also are given to other DoD organizations. The following have DoD Data Administration responsibilities as shown:

- a. ASD(C3I)
  - (1) Program Administration
    - (a) Act as senior information management official for the DoD.
    - (b) Prescribe and approve DoD data administration policies and procedures.
    - (c) Ensure development of DoD standard procedures.
    - (d) Designate a DoD DAd.
    - (e) Review and approve the DoD DASP submitted by the DoD DAd.
  - (2) Provide Technical Infrastructure
    - (a) Task the DASD(IM) to act on his or her behalf for information management issues.
    - (b) Task the DoD DAd to develop and administer standard DoD data administration products, procedures, and services.
    - (c) Ensure development and implementation of DoD standard data, logical data models, and tools.



(d) Ensure development, operation, and maintenance of a DoD data administration infrastructure.

(3) Operational Services

(a) Resolve data administration issues whenever possible and forward unresolved cross-functional issues with recommended actions to the ASD(C3I) for final disposition.

(b) Provide for the development and maintenance of the DoD Data Model and the DDRS.

b. OSD PSAs and the Chairman of the Joint Chiefs of Staff

(1) Program Administration

(a) Represent Functional Area interests to the ASD(C3I) and the DoD DAd.

(b) Review and approve planning, programming, and budgeting requirements for data administration within the Functional Area.

(c) Designate an FAd in each Functional Area for which they are responsible.

(d) Review and approve data administration plans (including action plans), in accordance with annual planning guidance, for the Functional Area(s) for which they are responsible.

(e) Execute the approved DoD DASP.

(f) Approve adjustments to Functional Area data administration action plans based on approved proposals for FPI, or due to ASD(C3I) guidance.

(g) Ensure Functional Area adherence to DoD data administration policies, procedures, and standards.

(2) Provide Technical Infrastructure

(a) Task the FAd to implement DoD Data Administration in each Functional Area for which they are responsible.

(b) Provide required data administration resources.

(c) Review and approve Functional Area(s) data requirements.

1 Approve Functional Area data requirements.

2 Review and approve Functional Area logical data models which are then sent to the Department of Defense for integration into the DoD Data Model.

3 Direct candidate and/or modified standard data elements be submitted to the Department of Defense for approval to meet Functional Area data requirements.

4 Implement approved changes to data.

(d) Establish internal procedures for data administration in their Functional Area(s).

1 Coordinate internal Functional Area data administration procedures with DoD data administration procedures.

2 Ensure compatibility between internal Functional Area data administration procedures and Functional Process Improvement (FPI) procedures.

(3) Operational Services

(a) Require the development and use of DoD standard data within the Functional Area(s) and in information systems developed to support the Functional Area(s).

(b) Ensure sufficient personnel are trained in data administration to support the needs of the Functional Area(s).

(c) Review the DoD Data Model as part of the approval process.

c. Component Heads

(1) Program Administration

(a) Represent Component interests to the OSD PSAs and the DoD DAd for all DoD data administration matters.

(b) Review and approve planning, programming, and budgeting requirements for data administration within the Component.

(c) Designate a CDAd to implement data administration procedures across all Functional Areas within the Component.

(d) Review and approve an annual data administration plan

(including action plans), in accordance with annual planning guidance, for the Component.

(e) Execute the approved DoD DASP.

(f) Approve adjustments to Component data administration action plans based on approved proposals for FPI, or due to ASD(C3I) guidance.

(g) Ensure Component adherence to DoD data administration policies, procedures, and standards.

(2) Provide Technical Infrastructure

(a) Provide required data administration resources.

(b) Review and approve Component data requirements.

1 Approve Component data requirements.

2 Review and approve Component logical data models which are then sent to the Department of Defense for integration into the DoD Data Model.

3 Direct candidate and/or modified standard data elements be submitted to the Department of Defense for approval to meet Component data requirements.

4 Implement approved changes to data.

(c) Establish internal procedures for Component data administration.

1 Coordinate internal Component data administration procedures with the Department of Defense and functional data administration procedures.

2 Ensure compatibility between internal data administration procedures and FPI procedures.

(3) Operational Services

(a) Require the development and use of DoD standard data within the Component and in information systems developed to support the Component.

(b) Ensure sufficient personnel are trained in data administration

to support the needs of the Component.

(c) Operate databases to support integrated operations and the use of shared DoD data resources.

d. DASD(IM)

(1) Program Administration

(a) Develop DoD data administration policies, and recommend the policies, the DoD data administration procedures, and related standards to the ASD(C3I) for approval.

(b) Review and recommend approval of the DoD DASP annually.

(2) Provide Technical Infrastructure

(a) Support the DoD DAd in acquiring the resources necessary to establish a DoD data administration infrastructure and implement the DoD Data Administration Program.

(b) Support development of DoD standard data, logical data models, procedures, and tools.

(3) Operational Services

(a) Act on behalf of the senior information management official on data administration issues, except for those issues needing ASD(C3I) resolution.

1 Review the DoD Data Model each time a new version has been approved.

2 Resolve conflicts not able to be solved by the DoD DAd.

(b) Facilitate the exchange of information relating to data administration products among OSD functional staff and Components.

e. DASD(IM) FIMs

(1) Program Administration

(a) Assist FDAdS in coordination of the Functional Area data administration plan, when requested.

(b) Review Functional Area data administration plan, and identify

and assist resolution of cross-functional issues.

(2) Provide Technical Infrastructure

(a) Facilitate coordination of data requirements across DoD Functional Areas.

(b) Support the development of DoD data administration products within and across Functional Areas.

(3) Operational Services

(a) Support use of DoD data administration products within and across Functional Areas and information systems used by the Functional Area(s).

(b) Support the training of sufficient personnel in the Functional Area(s) to implement the DoD Data Administration Program.

f. DoD DAd

(1) Program Administration

(a) Plan and budget for resources necessary to implement DoD Data Administration.

1 Identify resources needed to support DoD Data Administration activities conducted to meet the designated responsibilities for implementing data administration across the Department of Defense.

2 Plan and budget for resources consistent with the DoD Budget Guidance documentation.

(b) Establish requirements for models, methods, tools, data, and information technology.

(c) Develop and submit the DoD DASP to the DASD(IM) for final review and to ASD(C3I) for approval.

1 Coordinate DoD DASP Annual Planning Guidance with the DASD(IM).

2 Issue DoD DASP Annual Planning Guidance to FDAdS and CDAdS.

3 Receive and analyze FAdAd data administration plans from the OSD PSAs.

4 Receive and analyze CAdAd data administration plans from the DoD Components.

5 Consolidate FAdAd and CAdAd data administration plans into the DoD DASP, prioritize objectives, establish criteria, and align with Data Administration Program goals and available resources.

6 Develop DoD Data Administration Program action plans.

7 Submit DoD DASP to ASD(C3I) for approval.

(d) With coordination and assistance of FAdAds and CAdAds, develop DoD data collection, synchronization, and distribution plans based on the integration of functional and Component data requirements.

(e) Examine and evaluate current data collection, storage, and distribution technologies and make the information available to database administrators.

(f) Represent the ASD(C3I) and the DoD Data Administration Program to internal and external organizations on issues concerning data administration.

(g) Distribute the approved DoD DASP to FAdAds and CAdAds for execution.

(2) Provide Technical Infrastructure

(a) Acquire data administration resources.

(b) Implement DoD data administration standards, policies, and procedures.

(c) Develop DoD data administration procedures that specifically include procedures for data modeling, data standardization, data security, data quality assurance, and database operations.

(d) Develop the DoD Data Model.

(e) Facilitate implementation and use of DoD data administration procedures, tools, and standards.

(f) Develop a DDRS.

1 Collect user, functional, and technical requirements for a DDRS that are identified by FDAAd, CDAAd, and other DDRS users.

2 Develop logical data model for the repository that identifies all "critical" repository metadata.

3 Ensure that the logical data model and repository can be easily extended.

4 Establish configuration management procedures for the DDRS to manage functional and technical changes.

(g) Establish a DoD data administration training capability.

(3) Operational Services

(a) Implement and manage the DDRS. (Implement the DDRS to ensure efficient and effective operation of the repository and ensure appropriate users are able to access the system and the information it contains.)

1 Provide easy access and use of the repository by government and government contractor personnel within the level of classification and need-to-know.

2 Provide training for use of the repository.

3 Provide customer service.

4 Establish and chair the DDRS Configuration Steering Committee.

(b) Maintain the DoD Data Model.

1 Provide all services needed to manage and use DoD metadata stored in the repository.

2 Perform technical review and analysis of Functional Area and Component data models.

3 Coordinate with the FDAAd designated as the data steward to resolve functional and technical issues that were raised during the cross-functional review.

4 Review and approve or disapprove extensions or modifications to the DoD Data Model based on functional and technical evaluations.

5 Integrate approved data models, or data model views, into the DoD Data Model.

(c) Provide data administration customer service, education, training, and consultation.

(d) Provide standard data services.

1 Perform technical reviews of DoD candidate standard data.

2 Coordinate with the FDAAd designated as the data steward to resolve functional and technical issues that were raised during the cross-functional review.

3 Technically approve or disapprove DoD standard data.

4 Implement and enforce DoD standard procedures for data and database operations and maintenance.

(e) Provide for data security.

1 Specify security requirements for defense data handling facilities.

2 Execute secure data handling policies and procedures.

(f) Provide for data quality.

1 Specify quality requirements for Defense data handling facilities: e.g., information processing centers, megacenters.

2 Execute data quality policies and procedures.

3 Implement plans for data collection, synchronization, and distribution of DoD standard data.

(g) Perform configuration management on all DoD data products; e.g., DoD standard data, DoD Data Model, and the DDRS.

1 Establish and verify configuration baselines.



2 Determine the effect of change requests on configurations.

3 Ensure change control.

(h) Analyze use of DoD standard data, data security, and data quality to include data collection, synchronization, and distribution by evaluating trouble and/or discrepancy reports and complaints; and by conducting surveys and Program reviews.

(i) Conduct periodic Program assessments to evaluate progress and provide progress reports to the DASD(IM).

(j) Monitor and assess the progress of data administration action plan(s) implementation.

(k) Review, evaluate, and submit proposals for functional process improvement for the DoD Data Administration Program.

g. FDAAd

(1) Program Administration

(a) Serve as the Functional Area representative on functional issues affecting DoD Data Administration.

(b) Plan and budget for data administration resources within the Functional Area.

1 Identify data administration resources needed in the Functional Area.

2 Plan and budget for resources consistent with the DoD Budget Guidance documentation.

(c) Review, update, and prepare in coordination with the FAPMs, the Functional Area data administration plan in accordance with the DoD Data Administration Annual Planning Guidance.

1 Review DoD Data Administration Annual Planning Guidance.

2 Compile input to the Functional Area data administration plan, and submit the data administration plan to the OSD PSA.

3 Conduct Functional Area program assessments to evaluate progress.

4 Coordinate data administration plan with FAPMs.

(2) Provide Technical Infrastructure

(a) Acquire required data administration resources.

(b) Develop and ensure conformance of Functional Area data administration implementing procedures with DoD data administration procedures.

(c) Develop a logical data model for the Functional Area.

1 Reconcile data models and activity models developed by FAPMs in the Functional Area. (This includes resolving disputes among Components within the Functional Area whenever possible.)

2 Review and validate data models developed in the Functional Area.

3 Review and validate data requirements identified in the Functional Area data models for which data stewardship resides in another Functional Area.

4 Integrate approved data models across all functional activities within the Functional Area.

5 Coordinate, review, and approve extensions or modifications to the portions of the DoD Data Model for which they are steward.

6 Assist the DoD DAd in integrating approved data models or data model views (external schemas) into the DoD Data Model.

7 Maintain Functional Area data models in the DDRS.

(d) Assist data collection, synchronization, and distribution.

1 Document the single point-of-entry for data originating in the Functional Area.

2 Plan for the collection of functional data and coordinate with the DoD DAd.

3 Identify synchronization requirements of functional data to the DoD DAd.

4 Identify known data distribution requirements to the DoD DAd.

(e) Identify any functional requirements not provided by the DDRS and submit the requirements to the DoD DAd.

(f) Develop secure, quality, standard data in the Functional Area.

1 Establish standard data for use across the Functional Areas and in the DoD Components.

2 Use the DoD standard data element procedures to develop data elements for the Functional Area.

3 Develop Functional Area specific implementation procedures for data element standardization as necessary.

4 Utilize the DDRS to the maximum extent possible.

5 Ensure appropriate security requirements are identified for Functional Area data.

6 Ensure quality of standard data provided by the Functional Area.

### (3) Operational Services

(a) Conduct functional review of DoD candidate standard data for which they are designated as the data steward.

(b) Ensure staff is trained to carry out the DoD Data Administration Program within the Functional Area.

(c) Enforce use of DoD data administration policies, procedures, products, and standards within the Functional Area.

(d) Require and enforce use of DoD data administration products within the Functional Area by AIS PMs and the technical development activities that support the Functional Area.

(e) Require and enforce use of standard data in publications,

reports, records, messages, screens, and forms that are used and shared in the Functional Area. Exceptions may be granted by the FDAd when there is a compelling reason to allow deviation.

(f) Analyze the progress of Functional Area data administration action plans.

(g) Prepare and submit data administration progress reports to the DoD DAd upon request.

(h) Review, evaluate, and submit proposals for functional process improvements for data administration.

(i) Participate in all functional process improvement projects conducted in their Functional Area to provide oversight to data modeling efforts.

(j) Adjust action plans based upon approved functional process improvement proposals and DoD DAd guidance.

(k) Perform configuration management in the Functional Area.

1 Establish and verify data configuration baselines.

2 Determine the effect of change requests on data configurations (source collection and/or distribution).

3 Ensure change control.

h. CDAAd

(1) Program Administration

(a) Serve as the Component representative on Component issues affecting DoD Data Administration.

(b) Plan and budget for data administration resources required within the Component.

1 Identify data administration resources needed in the Component.

2 Plan and budget for resources consistent with the DoD Budget Guidance documentation.

(c) Review, update, and prepare the Component data

administration plan in accordance with DoD Data Administration Annual Planning Guidance.

- 1 Review DoD Data Administration Annual Planning Guidance.
- 2 Compile Component data administration plan and submit it to the Component Head.
- 3 Conduct Component program assessments to evaluate progress.
- 4 Coordinate data administration plan with functional personnel in the Component.

(d) Determine requirements for data collection, synchronization, and distribution.

- 1 Plan for the collection of Component data and coordinate with the FAd(s) and the DoD DAd.
- 2 Identify Component synchronization requirements of data and coordinate with the data steward(s) and the DoD DAd.
- 3 Coordinate known data distribution requirements with the FAd(s) and the DoD DAd.

(2) Provide Technical Infrastructure

- (a) Acquire required data administration resources.
- (b) Develop and ensure conformance of Component data administration implementing procedures with DoD data administration procedures.
- (c) Develop a logical data model for the Component.
  - 1 Reconcile data models and activity models developed in the Component.
  - 2 Review and validate data models developed within the Component.
  - 3 Integrate approved data models across all functional activities within the Component.

4 Propose extensions or modifications o the DoD Data Model to accommodate Component requirements.

5 Assist the DoD DAd in integrating approved data models or data views (external schemas) into the DoD Data Model.

6 Maintain Component data model in the DDRS.

(d) Conduct data collection, synchronization, and distribution.

Coordinate with the data steward(s) and the DoD DAd on the designation of the single point-of-entry for data originating in the Component.

(e) Identify any functional requirements not provided by the DDRS and submit the requirements to the DoD DAd.

(f) Develop secure, quality, standard data in the Component.

1 Establish standard data for use across the functional areas of the Component and among DoD Components.

2 Use the DoD standard data element procedures to develop data elements for the Component.

3 Develop Component specific implementation procedures for data element standardization as necessary.

4 Utilize the DDRS to the maximum extent possible.

5 Ensure appropriate security requirements are identified for Component data.

6 Ensure quality of standard data provided by the Component.

(3) Operational Services

(a) Facilitate coordination of data requirements across the Component.

(b) Act as liaison between Functional Areas within the Component, and the FADs and the DoD DAd.

(c) Ensure staff is trained to carry out the DoD Data Administration Program within the Component.

(d) Enforce use of DoD data administration policies, procedures, products, and standards within the Component.

(e) Require and enforce use of DoD data administration products within the Component by AIS PMs and the technical development activities that support the Component.

(f) Require and enforce use of standard data in publications, reports, records, messages, screens, and forms that are used and shared within the Component. Exceptions may be granted by the CDAd when there is a compelling reason to allow deviation.

(g) Require and support database administrators in the Component to physically implement that portion of the DoD Data Model required by users of a database.

(h) Analyze the progress of Component data administration action plans.

(i) Prepare and submit data administration progress reports to the DoD DAd upon request.

(j) Review, evaluate, and submit proposals for functional process improvements for data administration.

(k) Participate in all functional process improvement projects conducted in their Component to provide oversight to data modeling efforts.

(l) Adjust action plans based upon approved functional process improvement proposals and DoD DAd guidance.

(m) Perform configuration management in the Component.

1 Establish and verify data configuration baselines.

2 Determine the effect of change requests on data configurations (source collection and/or distribution).

3 Ensure change control.

i. FAPM

(1) Program Administration

Assist FDAAs in coordination and development of the Functional

Area data administration plan.

(2) Provide Technical Infrastructure

Assist the FAd in the development of the Functional Area data model and validate that functional data requirements of the functional activity model(s) are completely and correctly represented in the model.

(3) Operational Service

(a) Assist the FAd in maintenance of the Functional Area data model.

(b) Require information system and application software program development to use DoD standard data elements, and have candidate standard data elements developed when they do not exist already.

j. Database Administrators

(1) Provide Technical Infrastructure

(a) Develop and maintain physical data models based on the approved logical data models.

(b) Develop and maintain database structure using approved data entities and attributes.

(2) Operational Service

(a) Physically implement that portion of the logical DoD Data Model that is needed to support the users of his or her database.

(b) Coordinate database development with appropriate FAd and CDAs; i.e., functional staff and Components that use or need knowledge of the database.

(c) Use standard entities and attributes in database development and maintenance.

(d) Produce and disseminate database documentation.

(e) Provide technical assistance in the design of logical data models.

(f) Operate and maintain a database.



(g) Perform data quality analysis to detect and prevent data defects before they corrupt databases or end-user applications.

(h) Ensure data security measures are taken to prevent unauthorized access to the databases or changes to the data in them.

k. Technical Development Activities

(1) Provide Technical Infrastructure

(a) Use existing logical data model(s) when building an information system or an application software program and recommend modification to existing data models as new data requirements are identified .

(b) Provide the data model (view and/or subset of functional models or the DoD Data Model) to the AIS PM, and to the FDAAd or CDAAd for which the system and/or application is being developed.

(c) Help develop DoD candidate standard data to meet information system and/or application software program data requirements when no standard already exists.

(2) Operational Services

(a) Use DoD standard data elements in information system and application software program development.

(b) Work with database administrators in the design and implementation of physical databases.

I. AIS PM (This refers to any principal officials responsible for directing activities during concept exploration, definition, demonstration, validation, development, production, and development life-cycle phases of an information system, automated or non-automated.)

Operational Services

(1) Require and ensure use of DoD data administration products in the information system life-cycle. Exceptions to the use of DoD data administration products must be approved by the responsible FDAAd or CDAAd. Exceptions will be granted only when there is a compelling reason to allow deviation.

(a) Ensure use of DoD standard data and structures.

(b) Ensure development and maintenance of physical data

models using approved logical data models.

(2) Ensure implementation and maintenance of data quality requirements in the information system.

(3) Ensure security measures are taken to prevent unauthorized access to data in the information system.

m. Functional Users (to include end-users, action officers, and decision-makers at all levels)

(1) Provide Technical Infrastructure

(a) Develop or propose changes to data models to support new or changing business requirements.

(b) Develop DoD candidate standard data elements to meet data requirements when no standard data element already exists.

(2) Operational Services

(a) Use DoD standard data to meet data requirements.

(b) Assess the usefulness and benefits of the functional data requirements within information systems and recommend changes.

(c) Forward data discrepancies or problems to the FDAAd or CDAAd.

## CHAPTER 3

### PROCEDURES FOR PROGRAM ADMINISTRATION

#### A. INTRODUCTION

Program Administration refers to the oversight and management process necessary to manage data administration across the Department. The products of this main activity are data administration policy, plans, and requirements.

#### B. PROVIDE POLICY

##### 1. Establish Data Administration Policy

a. Description: This activity establishes a common set of rules and guidelines, which provide specific instructions by which the DoD Data Administration Program will be implemented and operated throughout the Department of Defense.

b. Purpose: To ensure a common understanding of how the DoD Data Administration Program will operate and to provide a framework within which data administration decisions can be made.

c. Inputs:

(1) DoD Directive 8000.1 (reference (g))

(2) DoD Directive 8320.1 (reference (c))

(3) DoD Directive 8120.1 (reference (b))

(4) DoD Directive 3405.1 (reference (m))

(5) DoD information requirements

d. Output: An established set of rules and guidelines that provide for specific instructions by which DoD data administration will be implemented and maintained.

e. Activities: Create the set of rules by which the DoD Data Administration Program shall operate.

2. ASD(C3I) establishes and provides overall direction and guidance for the DoD Data Administration Program. The ASD(C3I) also shall provide procedures for implementing and maintaining the DoD data administration infrastructure. Component

Heads and OSD PSAs shall provide more specific guidance to organizations under their control, consistent with the direction provided by the ASD(C3I). The reasons for having more generalized direction at the highest level is that no Department-wide procedures can possibly acknowledge all the different circumstances that may exist across a department as large and complex as the Department of Defense. The procedures developed at the highest level establish a framework within which the individual Component Heads and OSD PSAs may customize direction for implementation to fit their individual circumstances, as long as it is consistent with the higher-level policy. (See Figure 3-1, below.) The Components should establish subordinate functional data administrators to ensure functional coordination within the Component and to lend subject matter expertise to the FDAdS.

### C. DETERMINE REQUIREMENTS

#### 1. Establish, Approve, Implement, and Maintain Requirements for Models, Tools, Methods, Data, and Information Technology Function

a. Description: This activity develops and promotes DoD requirements for models, tools, methods, data, and information technology including data configurations, data quality, and data security. This includes data collection, storage, synchronization, and distribution requirements.

b. Purpose: To directly facilitate integrated operations and data sharing by identifying DoD-wide standards and practices.

c. Inputs:

- (1) Existing internal and external requirements.
- (2) Existing internal and external procedures.
- (3) DoD Directives and Instructions.

d. Outputs: Requirements for models, tools, methods, data, and information technology.

e. Activities:

- (1) Establish requirements for models, methods, tools, data, and information technology.
- (2) Approve and implement requirements.
- (3) Maintain requirements.

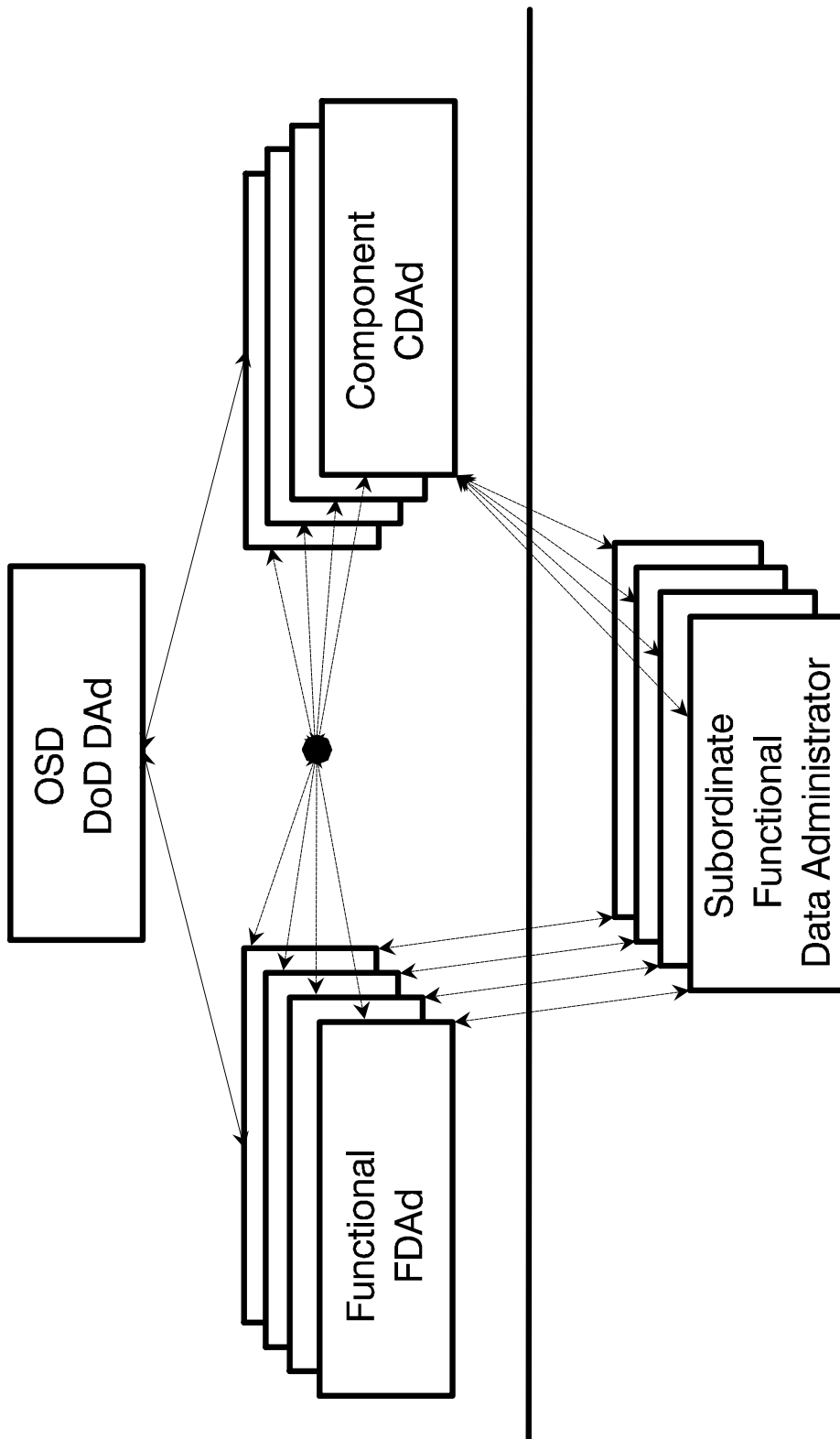


Figure 3-1: DoD Data Administration Framework

## Establish Requirements

a. The DoD DAd establishes requirements for models, methods, tools, data, and information technology. This process involves developing, approving, installing, supporting, maintaining, and updating the requirements.

b. Development of these requirements is based on internal and external existing standards, current technology, and current DoD procedures. Higher level standards (e.g., federal, national) shall be used whenever possible. FDAd and CDAd should provide their input to this process.

c. The DoD DAd, FDAd, and CDAd must ensure that requirements for data quality, data security, data collection, data synchronization, data storage, and data distribution are identified and documented for all data elements.

(1) To ensure data quality, data quality requirements and metrics must be established. Data quality requirements are defined from various authoritative sources during the identification and standardization phases of the data life-cycle. Data quality management is based on the principals of Total Quality Management as described in the "Total Quality Management Guide" (reference (n)). The DoD DAd, FDAd, and CDAd must ensure that data quality requirement are identified for all data elements. These requirements are documented in data administration products such as data models, the DDRS, and reverse engineering documentation.

(2) Data security requirements are specified in various directives such as DoD Directive 5200.28 (reference (i)). (See DFARS 227.4 (reference (o)) for security requirements applicable to purchased data marked with restrictive legends.) It is the responsibility of the DoD DAd, FDAd, and CDAd to ensure that the directions are understood and that data security measures are responsive and effective. (See Appendix F.)

(3) Data collection and synchronization requirements include the following issues: functionality (how data collection and synchronization supports the functional process), performance, compatibility, and auditability.

(4) To establish data storage and distribution requirements, the DBAd works with the AIS PM and the technical development activities to identify all existing and predicted future situations that will need data stored in the database.

d. Once the requirements for models, methods, tools, data, and information technology are established and in place, questions and conflicts inevitably arise. Therefore, the DoD DAd must support the requirements by providing users answers to their questions, and resolutions to any conflicts.

## 3. Approve and Implement Requirements

These requirements are functionally validated, then given to the DoD DAd for approval with DoD Directives and Instructions in mind. After the requirements are approved, they are installed, as appropriate, DoD-wide. The DoD DAd is responsible for publishing, promoting, and distributing these requirements and updating applicable regulations. Appendix A addresses life-cycle management of data that describes current data requirements.

#### 4. Maintain Requirements

a. To be effective and efficient, requirements must be maintained and updated on a regular basis to accurately reflect current circumstances. The FDAd and CDAd develop and revise action plans that reflect new, modified, and current requirements. These action plans are then documented in their Functional Area or Component data administration plans. The data administration plans are then integrated into the DoD DASP.

b. The Functional Area and Component data administration plans for the prior year serve as a baseline for assessing data administration requirements and measuring the effectiveness of the DoD Data Administration Program.

c. The DoD DAd measures the goals contained in the action plans of each Functional Area and Component data administration plan for the current year against the criteria established for each program goal in the DoD Data Administration Annual Planning Guidance and the DoD DASP for the prior year.

d. The DoD DAd provides the results of the evaluation, including program progress and direction, in the DoD DASP. This is the mechanism for submitting new requirements or for proposing modifications to existing requirements for models, tools, methods, data, and information technology.

#### D. PROVIDE STRATEGIC PLANNING

##### 1. Provide Strategic Planning

a. Description: This activity provides the comprehensive and long-term direction necessary to define, plan, implement, and operate the DoD Data Administration Program.

b. Purpose: To meet the requirements of an annual DoD Data Administration Plan for a successful data administration program as outlined in DoD Directive 8320.1 (reference (c)).

c. Inputs:

(1) Latest DoD Data Administration Annual Planning Guidance.

- (2) Latest Functional Area and Component data administration plans.
- (3) Latest DoD DASP.
- (4) New and revised policies and procedures.
- (5) New and changed requirements.
- (6) Current environment, including information technology infrastructure.

d. Outputs:

- (1) New DoD Data Administration Annual Planning Guidance.
- (2) New Functional Area and Component data administration plans.
- (3) Formal assessments of Functional Area and Component data administration plans.
- (4) New DoD DASP.
- (5) Known financed and unfinanced requirements.
- (6) Data collection, synchronization, storage, and distribution requirements.

e. Activities:

- (1) Provide DoD Data Administration Annual Planning Guidance.
- (2) Prepare and submit Functional Area and Component data administration plans.
- (3) Create, review, and approve new DoD DASP.

2. Provide DoD Data Administration Annual Planning Guidance

a. The DoD DAd in coordination with the DASD(IM) provides annual planning guidance to FDAdS and CDAdS by developing and issuing a memorandum. This memorandum initiates the coordinated data administration planning cycle, the major phases of which are aligned with the Program Objective Memorandum (POM) and DoD budget cycle.



b. The purpose of this annual planning guidance is to aid the FADs and CDAs in developing Functional Area and Component data administration plans, and planning and preparing budget submissions to resource data administration in their respective areas. This annual planning guidance provides the requirements, data administration program assessment criteria, schedule, and format for the new year DoD DASP.

c. The annual DoD DASP is the primary planning document that addresses and guides the development, implementation, and management of the entire DoD Data Administration Program. It is also the basis for determining the infrastructure requirements necessary to implement data administration activities in each of the Functional Areas and Components.

### 3. Prepare and Submit Functional and Component Data Administration Plans

a. Each FAD and CDA prepares a data administration plan for their respective Functional Area or Component in accordance with the DoD Data Administration Annual Planning Guidance provided by the DoD DAd.

b. The data administration plan prepared by each FAD and CDA is divided into two parts:

(1) Profile. The profile is an overview that provides introductory context and a summary of the Functional Area or Component plan.

(2) Action Plans. The action plans contain the goals, objectives, description of the tasks to be executed, major milestones, detailed resource requirements, and unresourced requirements for their respective areas. Estimates of resource requirements for each action plan should be prepared consistent with PPBS guidance.

c. Each FAD and CDA should consider migration system or process improvement initiatives in their respective Functional Area or Component when preparing a data administration plan. Functional Economic Analyses (FEAs), which facilitate the recognition and establishment of resource requirements, and information about the technical, as well as the functional, requirements for each area should also be incorporated into the data administration plan.

d. The FADs should coordinate with their FAPMs during preparation of the data administration plan.

e. Each FAD and CDA coordinates a completed data administration plan through their senior official (OSD PSA or Component Head) for submission to the DoD DAd for evaluation.

#### 4. Create, Review, and Approve New DoD DASP

a. After evaluating the Functional Area and Component data administration plans, the DoD DAd creates a draft of the DoD DASP for the new year by integrating the Functional Area and Component data administration plans and adding action plans specific to the overall DoD Data Administration Program.

b. The DoD DAd submits the draft DoD DASP for the next year, including a synopsis of each Functional Area and Component data administration plan, to the DASD(IM) for review and comment.

c. DASD(IM) submits the comments to the DoD DAd for reconciliation.

d. The DoD DAd submits the revised draft DoD DASP to the DASD(IM) for final review and forwarding to the ASD(C3I) for approval.

e. The DoD DAd distributes the approved DoD DASP to the FDAdS and CDAdS for execution.

#### E. DETERMINE RESOURCES

##### 1. Determine Resources

a. Description: This activity identifies the resources necessary to implement and operate DoD Data Administration.

b. Purpose: To plan for the acquisition of resources required to implement and maintain data administration activities.

c. Inputs:

- (1) Prior year action plans.
- (2) DoD DASP.
- (3) Current data administration activities.
- (4) Future data administration activities.
- (5) New and changed requirements.
- (6) Current information technology infrastructure.

d. Outputs:

(1) Known financed resource requirements.

(2) Known unfinanced resource requirements.

e. Activities: Determine financial, materiel, personnel, and data resources.

2. The FDAds and CDAds estimate personnel and procurement resources that will be required to fulfill their goals and objectives. FEAs facilitate the recognition and establishment of resource requirements, and information about functional and technical requirements.

3. Current fiscal year resources are identified to measure resource allocation shortfalls against budget requests.

4. Future fiscal year resources are identified to assist FDAds and CDAds in planning and preparing data administration related budget submissions in accordance with the POM and the Future Year Defense Plan (FYDP) procedures.

#### F. DEVELOP DATA ADMINISTRATION ACTION PLANS

##### 1. Develop Data Administration Action Plans

a. Description: This activity describes the resources, tasks, and milestones needed to implement and maintain data administration.

b. Purpose: To describe how a Functional Area or Component organization plans to meet identified data administration goals.

c. Inputs:

(1) Previous data administration action plans.

(2) Latest DoD Data Administration Annual Planning Guidance.

(3) Latest DoD DASP

(4) Resource requirements.

(5) Current data administration activities.

(6) Future data administration activities.

d. Outputs: Data administration action plans.

e. Activities: Develop data administration action plans.

2. Data administration action plans describe how a Functional Area or Component plans to meet identified data administration goals. There should be at least one action plan for each goal identified in the DoD DASP, including any data administration goals specified by the Functional Area or Component. Descriptive text for each action plan should include the goals and objectives supported, and associated major milestones.

3. Resource requirements must be provided for each action plan. Resource requirements document the estimated resources (manpower and funding) that will be required to fulfill each action plan. Unfunded resource requirements are identified to determine potential impacts from under-funding a specific activity.

## CHAPTER 4

### PROCEDURES FOR PROVIDING TECHNICAL INFRASTRUCTURE

#### A. INTRODUCTION

Technical Infrastructure refers to the internal framework that must be built to implement the Operational Services. The products of this main activity are data administration procedures, infrastructure, and tools.

#### B. ESTABLISH DATA ADMINISTRATION PROCEDURES

##### 1. Establish, Implement, and Maintain Procedures

a. Description: This activity develops and promotes the use of procedures that will guide the DoD Data Administration Program internally, and within Functional Areas and Components.

b. Purpose: To coordinate data administration activities and implementation across the Department of Defense, and ensure the goals and objectives established in the annual DoD DASP are achieved.

c. Inputs:

- (1) Internal and external standards.
- (2) DoD Directives, Instructions, and Manuals for information management, data administration, functional process improvement, and AIS life-cycle management.
- (3) Common tools to be used.
- (4) Functional process improvement "To Be" activity and/or data models.
- (5) Data administration plans.

d. Outputs:

- (1) DoD data administration procedures.
- (2) Functional Area data administration procedures that support the DoD data administration procedures.
- (3) Component data administration procedures that support the DoD

data administration procedures.

e. Activities:

- (1) Establish data administration procedures.
- (2) Approve and implement data administration procedures.
- (3) Maintain data administration procedures.

2. Establish Data Administration Procedures

a. DoD data administration procedures implement the concept of operations for data administration. These procedures must be developed, approved, installed, supported, maintained, and updated following DoD 5025.1-M (reference (p)).

b. DoD Directive 8320.1 (reference (c)) is the baseline document used in developing the DoD data administration procedures. Approved Component and Functional Area internal requirements for models, methods, tools, data, and information technology and the development of information that fits these requirements are incorporated into these procedures with any recommendations for improvements.

c. Since DoD data administration procedures are the overall guiding force for data administration, questions and conflicts that arise must be resolved in a timely manner to ensure efficient and effective data administration. The DoD DAd provides answers and resolutions to the Department.

d. The DoD data administration procedures are used as a baseline when developing the Functional Area and Component data administration implementation procedures. The Functional Area and/or Component procedures not only support the DoD data administration procedures, but they address specific internal activities such as review and approval procedures. DBAds establish procedures which support the implementation, use, and continuity of an effective education program, including formalized training. The areas of database concepts, database design, effects of database operation, database standards, efficient database usage, and high-level languages are addressed.

3. Approve and Implement Data Administration Procedures

Once Functional Area, Component, and DoD data administration implementation procedures are developed, they are reviewed and approved by the OSD PSAs, Component Heads, and the DASD(IM), respectively. The procedures are then installed, published, and distributed as appropriate. Copies of Functional Area and Component procedures must be sent to the DoD DAd within 30 days of publication.

#### 4. Maintain Data Administration Procedures

All procedures will be updated and maintained on a regular basis to accurately reflect the current circumstances. The DoD DAd, FDAd, and CDAd are responsible for evaluating the procedures and for providing recommendations for maintenance and updates.

### C. ESTABLISH THE DEFENSE DATA REPOSITORY SYSTEM (DDRS)

#### 1. Develop, Implement, and Maintain the DDRS

a. Description: This activity develops and operates the DDRS for all DoD metadata and other reusable information from which applications and databases will be developed.

b. Purpose: To facilitate data sharing and integrated operations of systems by providing access to standard metadata.

c. Inputs:

- (1) Functional requirements.
- (2) Technical requirements.
- (3) Operational requirements.
- (4) Personnel requirements.

d. Outputs:

- (1) The DDRS.
- (2) User support service.
- (3) Documentation.

e. Activities:

- (1) Develop the DDRS.
- (2) Implement the DDRS.
- (3) Maintain the DDRS.

#### 2. Develop the DDRS

a. The DDRS will be developed by the DoD DAd using the requirements defined by Functional Areas and Components. The functional requirements should be submitted to the DoD DAd by the appropriate FAd or CAd. Appendix C discusses data administration tools, requirements, and applications.

b. A model of the repository is then developed that accommodates new information and new requirements. The actual repository is developed from this model and therefore also accommodates new and/or revised information and requirements.

### 3. Operate the DDRS

The DoD DAd is responsible for the effective and efficient operation of the repository and for ensuring that appropriate users are able to access the system and the information it contains.

### 4. Maintain the DDRS

Maintaining and updating the repository to reflect current circumstances is another responsibility of the DoD DAd. As Functional Area and Component requirements change, recommendations for changes to the repository models or the repository itself are created. These change recommendations should be made through the appropriate FAd or CAd to the DoD DAd. The DoD DAd will use a Configuration Steering Committee with representation from all user communities to assist in identifying and prioritizing repository requirements. The DoD DAd reviews these recommendations and then oversees the implementation.

## D. ACQUIRE RESOURCES

### 1. Acquire Resources

a. Description: This activity acquires and uses necessary funds and manpower authority to fulfill resource requirements as identified in the DoD DASP.

b. Purpose: To provide the resources required to implement the data administration action plans.

c. Inputs:

(1) New DoD DASP.

(2) PPBS guidance.

d. Outputs:

(1) Program Objective Memorandum (POM).



(2) Fulfilled resource requirements (financial, materiel, personnel and data).

e. Activities:

- (1) Compile resource requirements.
- (2) Obtain funding and manpower authority.
- (3) Obtain resources.

2. Compile Resource Requirements

The DoD DAd, FADs, and CADs identify resource requirements for their respective area consistent with the DoD budget guidance documentation.

3. Obtain Funding and Manpower Authority

All DoD funding is obtained through the PPBS (reference (q)). The PPBS process is a cyclical, biennial process used to develop a plan, a program, and a budget for the Department of Defense. The PPBS provides a framework for making decisions on current and future programs through interrelated phases, consistent with national security objectives, policies, and strategies.

4. Obtain Resources

Manpower authority and funding are used by the DoD DAd, FADs, and CADs to obtain the resources required to build the technical infrastructure and perform the operational services for data administration in their areas. Funds are used to hire personnel, purchase materiel, and procure contractor services outlined in the approved DoD DASP, and Functional Area and Component data administration plans.

E. DATA MODEL DEVELOPMENT, APPROVAL, AND MAINTENANCE

1. Model Development, Approval and Maintenance

a. Description: This activity develops, approves, and maintains data models within the Department of Defense. (See Appendix D.)

b. Purpose: To provide the correct framework from which standard data are developed and to identify opportunities for improving data administration activities.

c. Inputs:

- (1) Activity models.
  - (2) Data requirements.
- d. Outputs: Data models.
- e. Activities:
  - (1) Develop data models.
  - (2) Approve data models.
  - (3) Integrate data models.
  - (4) Maintain data models.

2. The DoD Enterprise Model (reference (k)) is a representation of the activities and data of the Department of Defense, and the data component is a strategic level view of the DoD Data Model. The DoD Data Model extends down to the level of data entities, attributes, and relationships in concert with the definition of more detailed DoD activities. The fundamental objective of the DoD Data Model is to provide the basic data architecture for effective data administration across the Department. The DoD Data Model together with the DoD Activity Model comprise the DoD Enterprise Model. The DoD DAd is responsible for the development, approval, integration, maintenance, and extension of the DoD Data Model.

3. To implement data administration in a Functional Area or Component, data models must be developed, approved, and managed to accurately reflect the data in the Functional Area or Component. FDAdS and CDAdS are encouraged to communicate with the DoD DAd early in the modeling life-cycle to accelerate integration into the DoD Data Model.

#### 4. Develop Models

Data model development normally begins with activity modeling, which is covered in the ASD(C3I) Memorandum (reference (h)). Using activity models as a guide, data models are developed to reflect "as is" and "to be" functional data requirements. While "as is" models may not comply with standards, the "to be" models must adhere to DoD data modeling and naming standards. The creation and refinement of activity models and data models is an iterative process. The models are developed by the FDAdS and CDAdS in conjunction with the FAPMs and the Component personnel in charge of functional activities within the Component. The models are then reviewed, coordinated, and approved by the respective OSD PSA or Component Head. Cross-functional coordination is performed with the assistance of the DASD(IM) FIMs. These data models should then be submitted to the DoD DAd

using the DoD standard presentation language called the Integrated Computer-Aided Manufacturing Definition (IDEF) language. IDEF0 (IDEF zero) and IDEF1X (IDEF one x) are the DoD standard presentation styles used for activity and data modeling.

5. Approve Models

Approval of data models is given by the FDAd who act as representatives of the OSD PSAs, the CDAd who act as representatives of the Component Heads, and the DoD DAd who ensures cross-functional coordination.

6. Integrate Models

After approval, the data model is integrated into the DoD Enterprise Data Model by the DoD DAd with consultation of the FDAd, CDAd, and the DASD(IM) FIMs. This integration provides for data sharing and ensures integrated operations can be performed.

7. Maintain Models

Management of data models includes updates to these models made by the FDAd/FAPM and CDAd/Component functional activity expert teams to accurately reflect process and data improvements. As new information requirements are identified, the DoD Data Model will continue to change causing data entities, attributes, and relationships to be added, modified, or archived. FDAd and CDAd will ensure implementation of the updated standard data within their Functional Area or Component. Approved models are stored in the DDRS using tools and methods specified by the DoD DAd.

F. STANDARD DATA DEVELOPMENT, APPROVAL, AND MAINTENANCE

1. Data Standardization

a. Description: This activity develops DoD standard data using models. (See Appendix E.)

b. Purpose: To create standard data which directly allows for horizontal and vertical sharing of data, and facilitate integrated operations.

c. Inputs:

- (1) Data requirements.
- (2) Data entities and attributes from data models.
- (3) Data standardization policies and procedures.

- d. Outputs:
  - (1) DoD standard data (e.g., standard data elements and data structures).
  - (2) Documentation of DoD standard data and metadata.
- e. Activities:
  - (1) Develop DoD candidate standard data.
  - (2) Submit and approve DoD candidate standard data in accordance with procedures.
  - (3) Document and maintain DoD standard data descriptions in the DDRS and data element values in databases.

## 2. Develop Candidate Standard Data

Candidate standard data are developed using approved, integrated data models. Standard data elements are driven out of these integrated data models as described in the DoD "Data Element Standardization Procedures" (reference (f)). The data elements reflect data pertinent to that Functional Area or Component and are developed and documented by the FAd's and CAd's staff.

## 3. Submit and Approve Candidate Standard Data

Preliminary reviews of the candidate standard data and metadata are conducted by the appropriate FAd or CAd. The FAd or CAd will ensure that the information adheres to technical and functional requirements. This review process is specified by the FAd/CAd in an internal data administration implementation procedure document. Formal technical and functional reviews are conducted by the DoD DAd and FAd's, respectively; FAd's must, therefore, develop a formal functional review procedure. DoD DAd technical approval and FAd functional approval will result in the candidate standard becoming approved standard data. The DDRS supports the approval process electronically.

## 4. Document and Maintain Standard Data

The DDRS supports the development and maintenance of descriptions of standard data elements, data entities, data structures, and metadata. FAd's and CAd's will submit data entities and attributes to DISA for standardization and DoD approval. Also, to maintain data integrity and to preserve interfaces when changes occur to standard data, FAd's and CAd's will ensure registration in the DDRS of the information systems using standard data. This information also will be used to

determine if the proposed change is cost-effective. Development, approval, and management of standard data elements is further explained in DoD Manual 8320.1-M-1 (reference (f)).

## G. ACQUIRE COMMON TOOLS

### 1. Acquire Common Tools

a. Description: This activity develops and supports the acquisition of common tools.

b. Purpose: To directly facilitate integrated operations and data sharing through the use of DoD-wide standard tools.

c. Inputs:

- (1) Functional requirements.
- (2) Technical requirements.
- (3) Operational requirements.
- (4) DoD Directives and Instructions.
- (5) Data administration plans.
- (6) Operational tests and evaluations.
- (7) Standards.

d. Outputs: Common tools.

e. Activities: Acquire common tools.

2. To facilitate integrated operations and data sharing, common tools must be acquired and used. (See Appendix C.) Common tools will include, but are not limited to, a common repository, standard interfaces to that repository, information engineering tools, and data quality assurance tools. Architectural standards for data will guide the information system design process, and automated tools will support the reuse of data and software. Data administration products and services will be used extensively to meet the requirements of new information system development and will result in reduced development cost and time.

3. To maintain a common tool infrastructure, licensing, installation, and distribution of software and supporting documentation will be acquired and managed.

## H. ACQUIRE DATA COLLECTION, DISTRIBUTION, AND STORAGE CAPABILITY

### 1. Acquire Data Collection, Distribution, and Storage Capability

a. Description: This activity develops and supports the acquisition of collection, distribution, and storage capabilities.

b. Purpose: To control and maintain the flow of data into, within, out of, and among various databases; to control how, where, and in what manner, data is stored and maintained within each database and among databases.

c. Inputs:

(1) Policies and requirements gathered and integrated by the DoD DAd, FADs, and CDAs from users throughout the Department of Defense.

(2) Logical data models.

(3) Information technology infrastructure resources.

(4) Recommendations from computer operators, system developers, vendors, and users.

(5) Approved user processing and product requirements.

d. Outputs:

(1) Physical data models.

(2) Subject area databases.

(3) Reusable database schemas.

e. Activities:

(1) Acquire data collection capability.

(2) Acquire data storage capability.

(3) Acquire data distribution capability.

### 2. Acquire Data Collection Capability

DBAs work with the FAd or CAd of the responsible organization to provide a data collection capability necessary to support the needs of the Department

of Defense. During the data collection stage the DoD DAd, FADs, and CDAs must coordinate with the technical development activity and DBAs to ensure that the data quality requirements are implemented properly in databases and application software. When quality edit checks do not exist in legacy systems, the data must be extracted and examined manually or downloaded and analyzed with a data quality tool designed to generate the necessary quality edit checks.

### 3. Acquire Data Storage Capability

Acquire the database and storage when not already available. The DBAd, under the management of the AIS PMs, will install and load databases. Once installation and preliminary quality assurance tests are completed, the DBAd notifies the appropriate FAd or CAd. DBAs have the responsibility for the operational implementation of databases, from designing the physical database schemas and user views to guaranteeing the integrity and efficiency of the data access activities. The AIS PM helps manage these responsibilities. The DoD DAd must work to ensure adequate capability exists in the Department of Defense to meet the totality of user requirements.

### 4. Acquire Data Distribution Capability

Acquiring the data distribution capability including, if necessary, the rights to release or disclose purchased data. The DBAd then evaluates alternatives to find the best solution for data distribution based on cost-analysis and estimated costs for prospective services. To provide data distribution, the ways to distribute data to the various users are determined. The DBAd then evaluates alternatives to find the best solution for data distribution based on cost-analysis and estimated costs for prospective services. The DoD DAd must work with other DISA Component and Functional Area personnel to provide the capability to distribute data among the DoD databases to meet user requirements.

## I. DEVELOP CUSTOMER SERVICE AND TRAINING PROGRAM

### 1. Develop Customer Service and Training Program

a. Description: The activity develops a customer service and training program to support DoD Data Administration across the Department of Defense.

b. Purpose: To ensure that DoD data administration personnel have the appropriate training and support to implement the DoD Data Administration program.

c. Inputs:

(1) Procedures.

(2) Requirements.

- (3) DoD Directives, Instructions, and Manuals.

- d. Outputs:

- (1) Training classes.

- (2) Customer Service.

- e. Activities:

- (1) Develop training classes.

- (2) Develop customer service program.

2. The DoD DAd will develop and offer training courses to support the skills needed for data administration. The DoD DAd will acquire the appropriate services necessary to advertise and provide training to untrained FDAds and CDAds. The success of this program will furnish a trained data administration community.

3. A customer service program will also be developed to aid Functional Areas and Components in their implementation of data administration. This program will ensure each user has knowledge of access to the repository, correct use of DoD data administration procedures, and the use of the data administration products.



## CHAPTER 5

### PROCEDURES FOR OPERATIONAL SERVICES

#### A. INTRODUCTION

Operational Services refer to the precise actions necessary to fulfill the mission of the DoD Data Administration Program and to the use of the data administration final products. The products of this main activity are standard data, managed data in databases, and personnel trained and educated in data administration.

#### B. MANAGE DATA ADMINISTRATION ACTION PLANS

##### 1. Manage Action Plans

a. Description: This process manages the acquired resources and tasks identified in data administration action plans. Data administration action plans describe the resources, tasks, and schedules for building the Technical Infrastructure and providing the Operational Services.

b. Purpose: To provide clear, concise, and cost-effective direction to recognize process improvements and adjust data administration action plans accordingly. To assist in prioritizing activities and resource allocation.

c. Inputs:

- (1) Acquired resources.
- (2) Approved data administration action plans.
- (3) Proposals for process improvement (Implementation Plans and FEAs).

d. Outputs:

- (1) Progress reports.
- (2) Adjusted data administration action plans.

e. Activities:

- (1) Monitor and assess progress of data administration action plans.
- (2) Report progress of data administration action plans.

(3) Adjust data administration action plans.

2. Monitor and Assess Progress of Data Administration Action Plans

a. Monitoring and assessing the progress of data administration action plans is essential to the success of the data administration activities in each Functional Area and Component, as well as to the success of the DoD Data Administration Program as a whole. Monitoring and assessing the progress of data administration action plans is the means through which the actual accomplishment of tasks is controlled (i.e., project management).

b. As the data administration action plans in the approved DoD DASP and Functional Area and Component data administration plans are implemented, the DoD DAd and each FAd and CAd evaluate their success in meeting the goals and objectives in their respective areas by monitoring and assessing the progress of the data administration action plans. The criteria for action plan assessments are provided in the DoD Data Administration Annual Planning Guidance memorandum prepared by the DoD DAd.

3. Report Progress of Data Administration Action Plans

a. Progress reports are generated as a result of monitoring and assessing the progress of the various tasks, schedules, budgets, contracts, etc. contained in the data administration action plans.

b. The DoD DAd periodically provides progress reports to the DASD(IM).

c. The DoD DAd may also request progress reports from the FAd and CAd, and provide feedback, as deemed necessary.

4. Adjust Data Administration Action Plans

a. Data administration action plans are adjusted based on results from DASD(IM) guidance or approved proposals for data administration process improvements. As a functional activity, data administration must implement the functional management process as described in the ASD(C3I) Memorandum (reference (h)).

b. The DoD DAd, the FAd, and the CAd are responsible for reviewing and evaluating proposals for process improvement for their respective areas (i.e. Implementation Plans and FEAs) before submitting them to their respective OSD PSA or Component Head for approval.

c. Approved proposals, as well as the direct DASD(IM) guidance resulting from the review of progress reports, are the basis for adjusting data administration

action plans throughout the fiscal year. The DASD(IM) may provide implementation guidance or recommend additional adjustments to the data administration action plans.

d. The DoD DAd, CDAdS, and FAdS may adjust data administration action plans as needed for their specific internal data administration activities.

e. Major adjustments to the DoD Data Administration Program action plans may cause adjustments to Functional Area and Component data administration action plans. Normally, FAdS and CDAdS are not required to resubmit adjusted data administration action plans; annual data administration plans are submitted as a requirement of DoD data administration planning. However, the DoD DAd may require a special submission of Functional Area and Component-adjusted plans to ensure that they enhance the area's performance and continue to support goals and objectives of the current DoD DASP's .

## C. CONDUCT DATA COLLECTION, SYNCHRONIZATION, AND DISTRIBUTION

### 1. Data Collection, Synchronization, and Distribution

a. Description: This activity manages data and metadata throughout its life-cycle by performing data configuration management, assessing data quality, providing data security, and providing for data collection, storage, and distribution. As a result, opportunities for improving data administration and other activities are identified.

b. Purpose: To provide accurate, timely, and shareable data.

c. Inputs:

(1) Data models.

(2) Standard data.

(3) Policies and requirements set by the DoD DAd, FAdS, and CDAdS.

(4) Information technology infrastructure resources.

d. Outputs:

(1) Accurate, timely, shareable data.

(2) Physical data models

(3) Subject area databases.

(4) Inputs to information system planning.

e. Activities:

(1) Provide data configuration.

(2) Provide data quality.

(3) Provide data security.

(4) Provide data collection.

(5) Provide data storage.

(6) Provide data distribution.

(7) Provide technical support for data collection, synchronization, and distribution.

## 2. Provide Data Configuration

a. Providing data configuration involves maintaining data configuration inventories, performing change assessment services, and controlling the data configuration change process.

b. The inventories of data configurations contain information about the logical and physical data models that reside in the DDRS. These data models are controlled by the appropriate FDAd and CDAd and are stored in the DDRS using the tools and methods specified by the DoD DAd. Updates to these data models are made as data and data relationships change through FPIs, requirement changes, or performance tuning.

c. Change assessment is performed when new data requirements are specified by proposed functional process improvements. FDAd and CDAd determine the impact of these proposed changes. The costs of accessing and using existing data or the cost of migrating the current systems to support the new data are determined and included in the FEA for the proposed FPI.

d. Control of the data configuration change activity resides with the FDAd in Functional Areas and with CDAd in Components, but it is actually database administrators and technical development activities who implement the changes to the data configurations, application software, and physical database schemas. FDAd and

CDAdS prepare a change plan to guide the AIS PM and the technical development activity in implementing these changes. The DoD DAd will arbitrate cross-functional and/or cross-Component conflicts.

### 3. Provide Data Quality

a. After data quality requirement are defined, the process of providing data quality is divided into three activities or steps:

(1) Measure data quality.

(2) Analyze data quality.

(3) Improve data quality.

b. DoD Data Administration must ensure that DoD operations and decision-making are supported with data that meets needs in terms of availability, accuracy, timeliness, and integrity. Therefore, FDAdS and CDAdS must provide the quality of data throughout the data life-cycle. (See Appendix A.) The define activity focuses on identifying data quality parameters and establishing metrics. The measure activity focuses on measuring and assessing the data quality. The analyze activity focuses on identifying root causes of errors, establishing a poor-quality costs baseline, and analyzing opportunities for improvement. The improve activity focuses on developing and executing improvement initiatives for correcting data defects, and recommending functional process improvement (FPI) initiatives.

c. Evaluate Data Quality Assurance Progress. Measurement, evaluation, and reporting are essential elements of managing data quality. These elements focus on the effectiveness of improvement efforts and identify areas for future improvement efforts. The DoD DQE methodology provides the DAd with a means for identifying and assigning responsibility for corrective actions. A data quality baseline is always established in a DQE effort. The DAd can then use the baseline to assess progress toward achieving data quality by conducting periodic, identically configured DQE evaluations on the database. This provides a comprehensive indication of compliance with the quality requirements and reduced cost over a specified time period. When evaluating cost, there must be a determination of what is the acceptable percentage of defect data (target parameters) versus the cost of obtaining zero data defects. As part of the data quality assurance evaluation process, action plans should be reviewed by the DoD DAd, FDAdS, or CDAdS for the achievement of data quality assurance objectives and overall objectives for data quality should be reviewed and updated according to validated improvements. Finally, all procedures for data quality assurance should be re-evaluated.

d. Review, Approve, and Implement Data Quality Assurance Recommendations. Data quality recommendations may focus on developing and

executing Functional Process Improvement (FPI) initiatives to reduce future data defects. Any system and/or process defects found as a result of the DQE effort should be forwarded to the FAPM for correction. The FAPM should also identify and analyze root causes of data defects, identify opportunities for systems and/or process improvements, and prepare an implementation plan for approval in accordance with the ASD(C3I) Memorandum (reference (h)). All DoD employees will need to participate in implementing data quality improvement efforts. This reinforces the idea that managing data quality is not a program, but rather a new day-to-day behavior for the entire DoD.

e. The FDAdS and CDAdS must perform quality control activities to track corrections, inspect, and evaluate plans to ensure adequate quality control, and review format test plans to ensure that data quality is properly addressed. Once improvement recommendations are approved and executed, the data quality must be reanalyzed to measure improvements against the established baseline as part of a continuous improvement process for managing data quality. DBAdS also must conduct continued analysis to ensure data quality is being maintained, and correct any defects and or shortcomings detected or report them to the FAPM for corrections elsewhere.

#### 4. Provide Data Security

a. After data security requirements are established, providing data security involves two steps:

- (1) Implement security measures.
- (2) Perform security assurance evaluations.

b. Data security measures are implemented and enforced by DBAdS. They reconcile requests for access and other data security related issues and maintain the security level for each data element as documented in the DDRS or other published specific security documents.

c. Ongoing data security assurance evaluations are completed by FDAdS, CDAdS, and the DoD DAd to ensure that data security measures are enforced.

d. Provide data security at the operational level will include, but not be limited to, data backup and control of user identification and passwords. Control of user identification and passwords will include verification and authentication of user's need to know, user's clearance, and user's date of authorized access as well as the date the user is no longer authorized. When the data and/or database includes purchased data, control of non-government user access to the purchased data or software must be consistent with any use, release, or disclosure requirements applicable to the data or software.

#### 5. Provide Data Collection

Once the data collection capability has been acquired, the data undergoes quality assurance evaluations to verify that all requirements are met. The sources from which data have been acquired must be monitored to maintain an audit trail to introduce historical quality measures.

#### 6. Provide Data Storage

a. Once data are collected, the data must be maintained following the procedures for data quality and security. This ensures that the data can be accessed only by authorized users, and that the data are accurate and timely. DBAds are responsible for instituting procedures to track and document all changes to database-related items.

b. When data are no longer current, they are generally archived depending upon the requirements of the mission for which the data were used. The use of standard data in manual systems, forms, reports, messages, and publications must be considered before it is archived. Archived data, while not current, are still useful, and are sometimes required by law or regulation.

c. AIS PMs ensure that the data are archived in accordance with DoD 8320.1-M-1 (reference (f)). FDAdS will identify the data entities along with associated attributes and relationships that are no longer an information or functional requirement. The DoD DAd will establish the effective date for archiving the data and notify the registered users.

#### 7. Provide Data Distribution

After acquiring the capability for data distribution, the data is distributed to the various locations and/or individuals. The DBAd is responsible for this distribution which is managed by the AIS PM. The DBAd develops distribution strategies, using guidance from the DoD DAd that has been given to the appropriate Functional Area or Component, to change physical locations of data when required in response to mission activities such as troop deployment, technical infrastructure failures, or degradation that prevents acceptable availability or responsiveness of the data to a critical application(s). Loads on the networks due to access of data at particular locations are monitored and analyzed to keep the data distribution tuned to the distribution of applications using data. Based on the data distribution strategies and published guidance from the DoD DAd, the DBAd moves physical data when performance persistently stays below required availability and responsiveness levels.

#### 8. Provide Technical Support

a. DBAds have the responsibility for the operational implementation of databases, from designing the physical database schemas and user views to guaranteeing the integrity and efficiency of the data access activities. The AIS PM

helps manage these responsibilities.

b. The ultimate goal of database design is to produce a database at a minimum cost to users that supports maximum shareability of data and retains the integrity of the logical data model. The DBAd's goal is to provide the necessary design specifications for these physical databases. The design specifications include a physical data model based on the approved logical data model. The design process is iterative and involves trade-offs among performance, cost, and requirements. Any changes to the implementation of the logical data models would have to be documented and approved by the appropriate FDAd(s) or CDAd(s).

c. Implementation of the physical database schemas is completed by technical development activities in conjunction with DBAds and functional activities. This implementation includes creating the physical data structures on some storage medium, loading data values into those structures, and providing both appropriate access to, and security of, the database.

#### **D. PROVIDE CUSTOMER SERVICE AND TRAINING**

##### **1. Provide Customer Service and Training**

a. Description: This activity provides customer service and supports DoD Data Administration across the Department.

b. Purpose: To ensure correct and efficient implementation of DoD Data Administration.

c. Inputs:

- (1) Procedures.
- (2) Requirements.
- (3) DoD Directives, Instructions, and Manuals.

d. Outputs:

- (1) Personnel trained in data administration.
- (2) Personnel trained in database administration.

e. Activities: Provide customer service and training classes.

2. The DoD DAd is responsible for providing customer service and training to



the Functional Areas and Components to ensure that data administration is effectively and efficiently implemented. The data administration community is responsible for identifying training needs to the DoD DAd. FDAdS and CDAdS need to project training costs in their data administration plan.

#### E. USE DDRS

##### 1. Use DDRS

a. Description: This tool is used to support the administrators and users of the DoD Data Administration Program.

b. Purpose: To ensure a common tool and data for complete interoperability within the Department of Defense.

c. Inputs:

- (1) Data models.
- (2) Data elements.
- (3) Data entities.
- (4) Metadata values.

d. Outputs:

- (1) Standard data descriptions.
- (2) "As Is" Data Models
- (3) "To Be" Data Models

e. Activities: Use DDRS.

2. The DDRS is accessed and used by many members of the DoD data administration community to support their information and information systems needs. The DDRS will be used to disseminate data products to Component and Functional Area information systems and functional users (action officers and decision-makers) throughout the Department of Defense. Technical development activities will use the DDRS to identify DoD standards for use in AISs and application software.

3. The DDRS is used to:

- a. Research existing standard data, and/or submit proposed new standard

data.

b. Effectively facilitate the coordination of approved data standards across DoD organizations.

c. Resolve data standards conflicts.

## F. USE DoD DATA MODEL

### 1. Use DoD Data Model

a. Description: This product primarily is used to support the administrators of the DoD Data Administration Program.

b. Purpose: To map out the current and future organization and structure of data within the Department of Defense.

c. Inputs:

- (1) Data entities.
- (2) Data attributes (elements).
- (3) Information requirements.
- (4) Changing business needs.

d. Outputs: Organized and structured data capable of being reconfigured to suit changing business needs.

- (1) Standard data entities.
- (2) Standard data attributes (elements).
- (3) Relationships between data entities.
- (4) Standard data structures.

e. Activities:

- (1) Develop organized data.
- (2) Reverse engineer data.
- (3) Identify data entities, data attributes, and relationships among data

entities.

## 2. Develop Organized Data

The DoD DAd and the DAPMO will use the data component of the DoD Enterprise Model in developing organized and structured standard data entities and attributes capable of being reconfigured to suit changing business needs. To develop a data management strategy between the "As Is" data model(s) and the "To Be" data model(s), a series of target data models may need to be developed using the Enterprise Model as a "blueprint" for transition.

## 3. Reverse Engineer Data

FDAds and CDAds in conjunction with subject matter experts will use the DoD data model to reverse engineer nonstandard data into standard data consistent with the DoD Data Model. Input to a well-populated data model can be used to identify and re-engineer weaknesses in established or submitted data structures.

## 4. Identify Entities, Attributes, and Relationships

FDAds and CDAds identify data entities, data attributes, and relationships among data entities. These data entities and attributes are used to create standard data elements to be implemented in information systems and used in forms, publications, reports, records, messages, and screens. They are also used to link different Functional Area and Component data models to the DoD data model. Data entities and relationships are used to document and maintain business rules used by functional managers. FDAds, CDAds, and DBAds use data attributes to audit data values. When non-standard data is identified it will be forwarded to the responsible Technical Development Activity and DBAd for correction.

# G. USE STANDARD, QUALITY DATA

## 1. Use Standard, Quality Data

a. Description: This product is used to ensure unambiguous horizontal and vertical data exchange within the Department of Defense resulting in consistent decision-making.

b. Purpose: To support informed management decisions.

c. Inputs:

(1) Management inquiries.

(2) Standard data elements, entities, and structures.

d. Outputs: Integrated, consistent DoD decisions.

e. Activities: Use standard, quality data.

2. Standard, quality data are Goals Two and Four of the DoD Data Administration Program. (See section F. of Chapter 1, above.) Use of this product is critical to successfully implement horizontal and vertical, integrated data sharing within the Department. All members of the data administration community must strive to use standard, quality data whenever possible; and, even more importantly, strive to make standard, quality data available to decision-makers and action officers at all levels. Standard, quality data will be used in AISs, application software development, publications, forms, reports, records, and messages.

## H. USE EDUCATION, TRAINING, AND CONSULTATIVE SERVICES

### 1. Use Education, Training, and Consultative Services

a. Description: This service is used to acquire information and instruction about the DoD Data Administration Program.

b. Purpose: To inform FDAs, CDAs, DBAs, and customers about how to operate and maintain their portions of an integrated data administration program for the Department of Defense and make use of data administration products.

c. Inputs:

(1) Classroom training.

(2) Computer-based training.

(3) Directives, Instructions, and Manuals.

(4) FDAs, CDAs, DBAs, and customers.

d. Outputs: Trained personnel capable of confidently operating their portion of the DoD Data Administration Program.

e. Activities: Use education, training, and consultative services.

2. These products are used by FDAs and CDAs to inform and advise their personnel how to successfully run a data administration program within their respective organizations and functions. Classes cover a broad range of topics including overview

of the program, modeling, and data standardization; and are available in classroom or computer-based formats.

## I. USE COMMON PROCEDURES AND TOOLS

### 1. Use Common Procedures and Tools

a. Description: These products are used to support the unambiguous exchange of data within the Department of Defense.

b. Purpose: To ensure the unambiguous exchange of data within the Department of Defense.

c. Inputs: Common procedures and tools.

d. Outputs:

(1) Reused data models, information technology infrastructure, and application software.

(2) Timely and cost-effective information system development.

(3) Architectural standards for data to guide information systems design.

e. Activities: Use common procedures and tools as developed, designated, or made available by the DoD DAd and other data administrators and DBAds.

2. Common procedures and tools are used in much the same way, and for many of the same reasons, as standard, quality data: to successfully implement horizontal and vertical integration of data sharing within the Department. As with standard quality data, all members of the data administration community must strive to use common procedures (e.g., data administration manuals) and tools (e.g., software applications such as the DDRS, CASE tools, the DoD data model, re-useable software) whenever possible.

3. To support integration and consistency, the Department of Defense has approved the use of IDEF0 and IDEF1X for activity and data modeling as common modeling languages for the documentation of the Department's functions and data. They are both FIPS standards. (See reference (r) and reference (s).)

## APPENDIX A

### LIFE-CYCLE MANAGEMENT OF DATA

#### A. INTRODUCTION

1. DoD Directive 8320.1 (reference (c)) states that data administration "applies throughout the life-cycle of the ISs (information systems)" with management and acquisition reviews implemented by other referenced Directives. (See references (b), (t), (u), (v), and (w).)

2. Since an IS is often comprised of multiple subsystems, many or all of which may be at different phases of the life-cycle, the data administration function may be simultaneously involved in all phases of the IS life-cycle.

3. Data itself (once data and applications are separated in an AIS) has a life-cycle of its own separate from, but related to, the Automated Information System Life-Cycle (reference (b)).

The stages of the data life-cycle are:

- a. Identification
- b. Standardization
- c. Acquisition
- d. Maintenance
- e. Archival

4. An important aspect of the IS life-cycle is the identification and definition of the data requirements of the system. This aspect of the IS life-cycle is the primary focus of the data administrator.

#### B. IDENTIFICATION PHASE

1. The Identification Phase of the data life-cycle is known as strategic data planning. Strategic data planning determines the information requirements of the function necessary to perform its mission. Strategic data planning implements a technology-independent set of techniques to arrive at a set of data and activity models that represent the business of the enterprise. These techniques take into account the mission, goals, and objectives of the enterprise. Current systems are analyzed for input, output, and processes (forms, reports, and code) to assess the feasibility for

reverse engineering or re-engineering. The data models constructed act as a foundation for the development and definition of standard data elements. Thus, strategic data planning provides a framework where data become separate from their processes and constitute a resource independent of applications available for data use planning.

2. Strategic data planning is based upon the data requirements of specific functional processes performed in support of the Department of Defense's mission. Strategic data planning identifies the data required to satisfy specific information requirements in the most efficient manner. Data requirements also can be identified through less formal means such as system change requests.

### C. STANDARDIZATION PHASE

1. During the standardization phase, the information requirements identified through strategic data planning are given common or standard representations. The procedures for developing these standard representations are covered in detail in DoD 8320.1-M-1 (reference (f)). The standardization phase of the data life-cycle also addresses actual data values (items). There are many instances where the format and attributes of the data values must be standardized to ensure consistency across the Department of Defense (for example, the code length for the data element "Unit Identification Code" is different in each Service). When data must be shared by more than one functional activity, the standardization of data values is essential.

2. Strategic data planning establishes common data values and provides the framework for standard data use. It is in this area that the lines between standardization, acquisition, and maintenance become unclear. This is to say, once an information requirement is identified and the data elements representing that information requirement are defined, the data element domains may vary depending on usage.

3. The standards established in this phase will apply to information such as the authority for a specific instance of metadata, the preferred acquisition method and source for populating a database with a certain data element, the agency and/or organization responsible for the accuracy and/or integrity of the actual data values, and numerous other pieces of information. It is useful to view metadata as a type of controlling framework that outlines a broad set of rules to which the data of interest to an enterprise must be in compliance. The DoD DAd is the caretaker of this framework and its interface with the Department of Defense's overall mission. CDAd's perform the same functions within their own Components for their Component-level strategic data planning.

4. The final product of the standardization phase is the approved DoD standard data and metadata including data entities, attributes, definitions, and values. Applicable federal, national, and international data standards will be adopted as DoD

standards whenever possible.

#### D. ACQUISITION PHASE

1. Rules and standards governing acquisition and collection of data must be flexible enough to allow for varying data sources. The source and method of acquisition can have a significant impact on the reliability of the data. The quality and reliability of the data acquired must be measurable to allow for validation of the collected values. The sources from which data have been acquired must be monitored to maintain an audit trail to introduce historical quality measures.

2. Data to satisfy DoD information requirements may be obtained from an authoritative data source, designated in the standardization phase, (e.g., U.S. Postal Zip Code Directory for Zip Codes), from an external agent (other government agencies or commercial sources), some other means of direct collection (forms, monitoring devices, etc.), or it may be derived from other source data. An objective of Goal 2 of DoD Data Administration, a single point-of-entry for data, supports the designation of an external agent or database as the authoritative source for specific types and/or classes of data if such designation will reduce redundant collection efforts. A request to so designate may be submitted to the DoD DAd. The data from an authoritative data source, that is not subject to release or disclosure restrictions, must be made available to any user with a valid requirement and proper authorization. Authoritative source data subject to release or disclosure restrictions may only be released or disclosed on accordance with applicable restrictions.

#### E. MAINTENANCE PHASE

1. Once data are acquired by the Department of Defense, control must be exercised over its use. This phase involves ensuring that the data can be accessed only by authorized users, and that the data are accurate and timely. This is especially critical where the organization maintaining stewardship serves as the authoritative source of data for other applications and processes. The amount of time a data value spends in the maintenance phase is again dependent upon the requirements of the applications which use it.

a. If data are imported from outside the Department of Defense, a DoD point of contact must be assigned to ensure the data complies with the documentation requirements specified in the DDRS.

b. If data comes from within the Department of Defense, the functional data steward and the sole authoritative source of the data elements must work with the DoD DAd and the DBAd(s) to ensure the data complies with the documentation requirements specified in the DDRS.

2. Maintenance entails ensuring the integrity of the data in accordance with



guidance provided in the previous phases. Procedures for identifying authorized users are established by the data steward, and appropriate access controls are enforced through the implementing system(s). Data stewards are generally involved in all phases of the data life-cycle and serve as subject matter experts in the identification phase and as the designator of the authoritative source of data that spans all life-cycle phases.

#### F. ARCHIVAL PHASE

1. When data are no longer current, they are generally archived depending upon the requirements of the mission. For example, transactions in a payroll system are archived after a period of time to maintain a historical record. Archived data, while not current, are still useful, and are sometimes required by law or regulations.

2. Archived data must be allowed for use in time-series (trend) analysis.

## APPENDIX B

### INFORMATION ARCHITECTURE

#### A. INFORMATION ARCHITECTURES

An information architecture is a framework that portrays relationships among all data and activity components identified in models. It is an abstraction based on the products of the highest level of modeling and is further refined based on the next successive levels of modeling as each area of those detailed levels are completed. At the enterprise level, a strategic information architecture is derived from the enterprise model to identify broad information strategies that will be the basis for strategic data planning. Information architecture leads to the reduction and/or elimination of redundant and inconsistent data. Redundant and inconsistent data are difficult to identify and resolve when an information system, database, file, report, or form is viewed as an isolated collection of data. Separating data from application programs and placing them within logical groupings and precise structures permits the identification, reduction, and control of the redundancies and inconsistencies in data. This is a prerequisite for, and promotes, data sharing.

##### 1. Activity (or process) Architectures

An activity architecture is part of an information architecture. It is the framework for developing applications and defining their interrelationships in support of an organization's information architecture. An activity architecture is part of an information architecture. It identifies the major activities or processes an organization performs and their interrelationships.

##### 2. Data Architectures

a. A data architecture, another part of the information architecture, is a structured method for organizing data, and the information derived from that data, into manageable groupings to facilitate the shared use and control of that information throughout the organization. The data architectures provide the basis for the incremental, ordered design and development of systems and databases based on logical data models. (See Appendix D.)

b. A data architecture is derived from detailed data models. For instance, a strategic data architecture is derived from the enterprise model or strategic data model and shows the relationships among information classes (major groupings of related data) and depicts the fundamental data relationships among Functional Areas or partitions. The data architecture then is abstracted between stages of modeling and updated as the next levels of modeling are completed.

c. Data models and schema(s) are used to depict information needs or data requirements from a number of views. These views are typically mapped to one another to support the integration of strategic planning, business area planning, system requirements identification, and AIS design, development, and maintenance.

d. Three types of schemas are used to support various perspectives of an organization's data. The American National Standards Institute Standards Planning and Requirements Committee (ANSI/SPARC) has developed what is referred to as a Three Schema (Level) Architecture as described in NIST Special Publication 500-173 (reference (x)). The descriptions go well beyond the definitions for the three schemas contained in the Glossary in this Manual. The descriptions are included here for further understanding.

(1) Conceptual Schema. The conceptual schema represents the logical view, or data administrator's view, of the data requirement. This view is represented as a semantic model of the information that is stored about objects of interest to the Functional Area. This view is a single integrated definition of the data that is unbiased toward any single application of data and is independent of how the data is physically stored or accessed. An attributed, normalized data model is also referred to as a conceptual schema. The conceptual schema is used for data standardization and database design. It provides a consistent definition of the meanings and interrelationships of the data that is used to integrate, share, and manage the integrity of data within and across applications and user communities.

(2) Internal Schema. The internal schema represents the physical view or DBAd's view of the data requirement. This view is described by the data definition language (DDL) and physical storage methods used to implement the data requirements described under a conceptual schema. The denormalization of a conceptual schema may occur be required because of system performance and technological constraints. Any denormalization of the logical data model must be coordinated with the data administrator of the conceptual schema. The internal schema is also referred to as the physical data model. The design and development of internal schema(s) supports integration at the application and local levels.

(3) External Schema. The external schema represents the user view, or application view, of the data requirement. This view is represented by reports, transactions, and screens that are designed to support the individual worker, or groups of workers, in the performance of tasks or activities. The external schema is often referred to as the end-user view.

## APPENDIX C

### DATA ADMINISTRATION TOOLS

#### A. GENERAL

##### 1. INTRODUCTION

a. This Appendix provides information for selecting and using tools to support DoD Data Administration. The DoD Data Administration infrastructure is not linked to, or supported by, a particular commercial or internally developed information or software engineering methodology; however, it will support the use of commercial methodologies. Selection and use of any particular methodology will not be static. In accordance with FIP PUB 184, "Integration Definition for Information Modeling (IDEF1X)" (reference (r)), IDEF1X shall be used to integrate data models.

b. There are a variety of views of the scope of data administration and the methods to perform it. Some focus purely on the data in analysis and modeling; other methodologies recognize a strong link between activity and data analysis and modeling. Others say that data and activities should be integrated into an object-oriented approach. Whatever methodology is selected, it must emphasize the DoD-wide view of data, information system development, utilization and evolution of data and activities in existing systems, and collective integration of DoD data resources.

##### 2. TOOL CAPABILITIES

a. To date, there are a number of computer-aided software engineering (CASE) tools that support the full life-cycle, from analysis to code generation. The later system development phases, such as, system implementation and physical database design are supported by only a few, highly specialized tools.

(1) The majority of CASE tools support the early systems development phases, such as Strategic Systems Planning and Requirements Analysis. Such tools are popularly called front-end tools.

(2) The mid-level system development phases, such as System Design and Logical Database Design, are supported by a broad number of specialized CASE tools.

(3) The later system development phases, such as System Implementation and Physical Database Design, however, are supported by only a few, highly specialized tools. These tools, including code generators and fourth generation languages, are called back-end tools.

b. At a minimum, appropriate data administration tools should provide support for the following functions:

- (1) Project management.
- (2) Data dictionary services.
- (3) Activity and data modeling tools.
- (4) CASE tools.
- (5) Re-engineering and reverse engineering.
- (6) Database management.
- (7) Tools for data analysis, cross-referencing, and mapping of data in existing systems.
- (8) Data quality assurance tools.
- (9) Configuration management tools.
- (10) Tools to assist in data synonym and redundancy control.

### 3. METHODOLOGIES TO SUPPORT DATA ADMINISTRATION IN THE DEPARTMENT OF DEFENSE

a. Linking methodologies and tools currently being used throughout the Department of Defense is essential to the successful development of the data administration infrastructure. This will aid in the development and modernization of the Department of Defense's automated and non-automated information systems. Components should attempt to migrate to Component-wide (and ultimately, DoD-wide) common methodologies and sets of tools (e.g., information engineering and CASE tools) that conform to the following criteria as closely as possible:

- (1) Assist all DoD organizations to develop strategic, tactical, and operational data and activity models based on their mission, functions, goals, objectives, and enterprise strategies.
- (2) Link strategic planning, modeling of the plan, and management of the implementation of the plan together as a coherent functional activity.
- (3) Consist of a formal set of interrelated disciplines, procedures, techniques, deliverables, and quality assurance tests; and support the entire data and information system life-cycle for organization strategic functional planning, and

requirements to data or information system replacement or retirement.

(4) Incorporate integration of data and activity analysis and modeling that ideally will be capable of evolving to support emerging methodologies and techniques.

(5) Be capable of using the same techniques and procedures on any size or complexity of organization or project.

(6) Be easy to learn, understand, and use by executive, senior, and middle functional managers and personnel as well as data processing personnel because it will be used to identify the management and functional requirements of the organization.

(a) This includes the use of the methodology to assist management in the development and maintenance of strategic, as well as tactical and operational plans.

(b) This includes the production of data, activity, and possibly object models and reports that managers, users, and technicians can easily understand and use.

(7) Facilitate the documentation, analysis, refinement, and development of enterprise rules through models and reports.

(8) Be capable of defining the data architecture.

(9) Be capable of defining the functional partitions in the enterprise, analyzing those partitions to identify databases, developing database plans, and guiding and overseeing the function of database administration.

(10) Be rigorous enough to link each succeeding methodological phase to each other and ultimately to the technical or physical environment in which the logical data models will be implemented.

(11) Control and document data redundancy and facilitate systems integration top-down.

(12) Maintain technological or physical independence throughout the logical stages of the methodology.

(13) Be capable of effectively supporting transition from the logical to the physical stages of the methodology.

(14) Support the creation, development, maintenance, and

management of flexible information systems that can be rapidly and readily modified.

b. Having the capacity to provide an organization-wide, top-down, shared data, business planning strategy also is essential. The Department of Defense should have those capabilities in the CASE tools it procures and uses.

## B. SPECIFIC

DoD Data Administration is supported primarily by the following tools:

### 1. Information Resource Dictionary System (IRDS) tools.

The fundamental tool to support Data Administration is the data dictionary. The terms data directory, data encyclopedia, and data repository are widely used in the same context as data dictionary, but no standard definitions are universally accepted. For the purposes of this Manual, all three support the concept of "a specialized database containing information about data, such as meaning, relationships to other data, origin, usage, and format, including the information resources needed by an organization."

a. An "encyclopedia" is more frequently used to reference the dictionary and directory features of CASE tools.

b. A "repository" denotes more robust functionality and includes full extensibility, versioning, security, and other specific services such as data model notation and metadata storage, diagram generation, and related services.

c. A "data directory" is defined by Federal Information Processing Standard (FIPS) 156 (reference (y)) as a subset of a data dictionary and/or directory that identifies data location and ownership.

(1) The DDRS is the data dictionary system which supports DoD Data Administration as specified in DoD Directive 8320.1 (reference (c)).

(2) The current IRDS standard (reference (y)) was established to support the development of automated tools which in turn will support the application of data administration data standards and procedures. The standard assumes no implementation environment and assumes no run-time or compile-time dependent interfaces. The DDRS will become conformant with the FIPS 156 (reference (y)) as the IRDS standard at the earliest possible date.

(3) Component and Functional Area data dictionaries will be logically integrated and consistent with the DDRS but may be separately implemented apart from the DDRS. At a minimum, the DDRS will serve as the "dictionary and clearinghouse" for DoD standard data elements that all DoD Components and

Functional Areas will be sharing to control and reduce redundancy and improve efficiency of database operations. The DDRS will evolve to support the more robust functionality.

d. The DDRS will:

- (1) Support metadata definition, description, and management including the cross-referencing of information.
- (2) Include schema extensibility, metadata analysis, and easy-to-use report generation.
- (3) Provide guidance to users on how to follow one or more of the selected commercial or developed methodologies in support of DoD Data Administration.
- (4) Provide support of users for metadata naming analysis and verification.
- (5) Provide a standard method and functionality to support metadata interchange.

## 2. Computer-aided Software Engineering (CASE) tools.

a. CASE tools are most often used to assist in analyzing and designing information systems. CASE tools provide a data element consistency check against the entries in the DDRS. These tools generally include graphical support for the activity-orientated functional requirements decomposition methods, and the data-centered information engineering methods.

b. Support for configuration management is provided by maintaining the traceability links from the data models to the functional requirements being satisfied by the application software under development. The software life-cycle can be supported by maintaining the actual application software program listings and generated code in the metadata dictionary along with the required documentation. When a fully integrated CASE tool is utilized in this manner, the functional processing requirements, data, models, database schema, software, and documentation are available electronically for reuse or modification. This facilitates the life-cycle maintenance of the requirements.

## 3. Other Tools.

There are other tools (whether considered CASE or not) that might assist in supporting the development of a successful infrastructure:



- a. A data element creation or assistance tool (generally custom built); i.e., if the data dictionary cannot check the data element naming conventions, a separate automated tool might be designed or acquired for that purpose.
- b. Reverse engineering and re-engineering data modeling tools. Reverse engineering tools can be used to develop data models where none exist.
- c. Data-related quality assurance tools.
- d. Fourth generation language and code generating tools.

## APPENDIX D

### INFORMATION MODELING

#### A. INTRODUCTION

1. Data and activity models must be developed to support planning and management activities for data, information, and activities required to achieve the mission and business goals and objectives of the Department of Defense. Data and activity models provide the link needed to unify functional planning, modeling, and implementation activities into a coherent organization or functional activity. These models are also used to develop and maintain DoD standard data elements.

2. Redundancies and inconsistencies in data and activities are difficult to identify when each organizational sub-component, information system, database, report, form, or user requirement is managed in isolation. Once data and activities can be viewed from an organization-wide perspective and placed in logical groupings, redundancies and inconsistencies can be identified, and data and process sharing can be achieved.

3. Data and activity modeling taken together are referred to as information modeling. Information modeling by approved methods will contribute to achieving Goal 3 of the DoD Data Administration Program, "Use of Common Procedures and Tools," which in turn will contribute to achieving Goal 4, "Quality Data." (See Section F. of Chapter 1, above.)

#### B. TYPES OF MODELS

1. The models needed to support any size, or complexity, of organization can be separated into two basic types:

a. Activity models.

(1) An activity model provides a framework for identifying, defining, and organizing the functional strategies, rules, and activities needed to manage and support the way an organization does, or wants to do, business. It provides a graphical and textual framework for organizing activities into manageable groupings to facilitate their shared use and control throughout the organization.

(2) While data models represent the data necessary to achieve the mission of the organization, activity models document the functional activities of an organization. Activity models also document the associations or relationships among primary items of information that are important to the organization. Activity modeling permits the development, consolidation, and use of the same functional activities

across multiple Functional Areas. As with data modeling, this approach can help control the duplication and repetition of functional activities. A functional activity can be modeled once and then made available to all potential users rather than each user separately designing, developing, and maintaining the same activity. Activity models also facilitate the reuse of automated applications.

(3) Rule modeling, which occurs within both the data and activity modeling, includes identifying, capturing, analyzing, refining, and documenting the business strategies, rules, and activities. Once identified and captured, business rules can be analyzed and refined. This may result in decomposition of a complex rule to multiple rules, discarding or refinement of a current business rule, or identification of a new business rule.

#### b. Data Models.

(1) A data model is a graphical and textual representation of analysis that identifies the data needed by an organization to achieve its mission, functions, goals, objectives, and strategies; and to manage and operate the organization. It describes the scope, boundaries, and types of data needed to support the functional activities at all levels of the organization.

(2) The data model identifies what data are shareable across functional and organizational boundaries, and what data are redundant and unnecessary. It provides the top-down, organization-wide perspective needed for planning, designing, building, and maintaining future integrated information systems with a single point-of-entry for the data and contains information about the business rules of the organization.

(3) Data modeling techniques and tools help management and other personnel to accurately plan, identify, represent, relate, standardize, and store the data needed by the organization.

### C. PURPOSE OF THE MODELS

1. The primary purpose of activity and data modeling is formal, structured analysis of how a function operates (or should operate), and what data and information is needed to accomplish the function's mission. Lower level models must reflect the model at the next higher level. Modeling supports effective and efficient implementation of a function's goals and objectives, its management strategies, and its functional practices. Modeling also helps managers to identify and evaluate improvements in goals and objectives, strategies, and practices. The disciplined analysis and documentation performed during modeling facilitates definition of information system functional requirements. In turn, this simplifies and accelerates system development, and helps to ensure that the deployed system meets user needs.

2. Activity and data models address the activities required to plan, design, model, synchronize, standardize, and control data used by functional activities at all levels. They can be used to develop more accurate software, information systems, and databases. Information systems that are developed using activity and data modeling techniques and tools are easier and more cost-effective to update and maintain as the functional requirements change.

#### D. ACTIVITY MODELING STAGES

The activity modeling methodology and tools selected will define the exact procedures to be used, but the following are the generally accepted stages of activity modeling:

1. Establishing the activity model scope (e.g., strategic, mid-level, operational) and obtain commitment of the senior organization official of the activities that are to be modeled.
2. Identifying and assembling an activity modeling team that has the functional activities, knowledge, and expertise. Personnel within the Functional Area with data modeling expertise should be part of the team.
3. Identifying and obtaining relevant documentation, such as standard operating procedures, technical manuals, and other documents that define and discuss the laws, policies, rules, practices, procedures, and activities that are employed to operate the function.
4. Conducting activity modeling training workshops.
5. Conducting activity modeling sessions to develop activity models.
6. Refining the activity models to directly support functional policies, rules and activities, and ensuring consistency with the data model being developed at the same time as well as consistency with higher level activity models.
7. Fully documenting the activity models.
8. Acquiring senior management's approval of the activity models.

#### E. DATA MODELING STAGES

The data modeling methodology and tools selected will define the exact procedures to be used, but the following are the generally accepted stages of data modeling:

1. Identifying and assembling a data modeling team. This must include members from the activity modeling team to ensure consistency and verification of

understanding of the activity model by the data modeling team.

2. Identifying and obtaining available relevant documentation, such as the organization's mission, functions, roles and responsibilities statements; strategic business management plan, if available; and other documents on the organization's business directions and plans.

3. Conducting data modeling training workshops.

4. Conducting data modeling sessions to develop data models using the activity models and higher level data models as a primary information resource.

5. Refining the data models to directly support mission, goals, objectives and functional strategies.

6. Fully documenting the data models.

7. Analyzing the data model to prepare priority and decision scenarios for implementation and for the next lower level modeling activity; e.g., strategic level analysis to identify functional partitions, building an enterprise data architecture, and developing a decision package to obtain priorities for order and timing of additional modeling based on the architecture.

8. Acquiring senior and other levels of management approval of the data models and obtaining direction and timing for modeling projects.

## APPENDIX E

### DATA STANDARDIZATION

#### A. PURPOSE

The purpose of this Appendix is to provide information on standardizing DoD data. It describes how data modeling is the key aspect of the DoD Data Administration Program that derives data for standardization. This Appendix further provides information for standardizing DoD data such as prime words, data elements, class words, and generic elements.

#### B. DATA STANDARDIZATION

1. Data standardization is achieved by logically identifying, grouping, and classifying data.

a. The DoD Data Model is a logical representation of DoD data and how it is categorized based upon information requirements. Prime words and data elements are derived from the logical grouping of data in either the DoD Data Model, or the Functional Area or Component Data Models. The purpose of this logical grouping is to define, name, and identify characteristics of data to eliminate redundancy and facilitate common use and understanding.

b. Once data requirements are identified, they are classified according to like structures and domains. The purpose of this logical grouping is to identify standard rules for creating, sharing, maintaining, manipulating, and representing like data. Class words and generic elements facilitate this physical grouping of data.

#### C. ROLE OF THE DoD DATA MODEL

1. Without an approved DoD Data Model, DoD standard data elements and their metadata cannot exist. As Functional Area and Component data models are developed and approved, they are used to extend the DoD Data Model. This process enables the evolution of the DoD Data Model to meet changing DoD mission and functional requirements.

2. The DoD Data Model shall be used to produce standard data and data structures (i.e., data entities, attributes, prime words, and data elements).

a. Approved data entities will yield standard prime words with assigned data stewards.

b. The attributes of approved data entities will produce candidate standard

data elements for approval via the "Data Element Standardization Procedures," (reference (f)).

3. The strategic level DoD Data Model as presented in the DoD Enterprise Model (reference (k)) can be used as the "blueprint" for transition from the "As Is" to the "To Be" DoD Data Model through a series of target data models which support a data management strategy for the Department of Defense.

#### D. PRIME WORDS

1. Prime words are centrally controlled and maintained by the DoD DAd. Prime words are the names of data entities in the DoD Data Model or derived from them. New prime words are approved based on the extension of the DoD Data Model.

a. Any person, either within the Department of Defense or representing a DoD organization, may propose to extend or update the DoD Data Model. The originator prepares a proposal package consisting of a logical, fully attributed, normalized, data model that depicts data entities, their attributes, and relationships. The originator submits the proposal package to their respective FAd or CAd.

b. The FAd or CAd conducts a preliminary review of the proposal package to ensure adherence to mandatory technical and functional requirements and to reconcile developmental data entities and attributes with the current DoD Data Model. Upon completion of the preliminary review, the FAd or CAd will submit the package for informal review to the FAd designated as the data steward, and to the DoD DAd.

c. The FAd, designated as the data steward, with guidance from the DoD DAd, will conduct an informal review upon receipt of the proposal package. The FAd and the DoD DAd will coordinate and perform concurrent functional and technical reviews. The FAd will track the status of the proposal and keep the submitting FAd or CAd informed of progress and results. The FAd should coordinate with their functional area experts, including FAPMs, OSD PSAs, and FIM to ensure that their requirements are fully represented. The FAd also is encouraged to discuss proposals with functional counterparts within Components, CAdS, the originator, and other FAdS. For accepted proposals, the FAd or CAd designates the accepted data entities as candidate or modified prime words via the DDRS and forwards the proposal package to the DoD DAd for formal approval.

d. The formal approval process consists of a technical and functional review and final approval. The purpose of the technical review is to ensure that data entities and attributes adhere to technical standards. The purpose of the functional review is to ensure that data entities and attributes are represented consistently, are commonly understood, and support DoD cross-functionally. The final approval consists of technical and functional approvals based upon the technical and functional reviews

and, if needed, mediation. The DAPMO technically approves, the FADs functionally approve, and the DoD DAd mediates.

2. Prime words and data stewards are determined for each approved data entity and stored in the DDRS to allow for data element standardization. Data elements are derived from approved data entity attributes and are approved via the "DoD Data Element Standardization Procedures," (reference (f)).

#### E. CLASS WORDS

1. A class word designates the category of data into which a data element fits. It establishes the general structure and format of data in the domain for that data element. Class words are reserved words that are used to categorize the data at its highest level. Approved DoD standard class words are recorded in the DDRS. They are centrally controlled, and maintained by the DoD DAd.

2. All data elements are required to fit into a category. If a new data element does not fit into a category then a proposal may be made to create a new category of data (class word). Proposals for new class words are submitted via an FAD or CDAd to the DoD DAd. The DoD DAd approves new class words base upon recommendations from FADs and DAPMO.

#### F. GENERIC ELEMENTS

1. A generic element is the part of a data element that establishes a structure and limits the allowable range of values of a data element. A generic element has no functional or application context other than to define a general class of data and to establish groups of data elements within the same class that have the same structure and related domains.

2. Generic elements are represented in the DoD Data Model as attributes that are used to define two or more different data entities (e.g., color name). When developing generic elements, it is important to analyze them via the data modeling process to ensure that it is not actually an attributive entity that the Department of Defense would like to keep information about (e.g., security classification code).

3. The generic element consists of a class word and, if necessary, modifiers that are derived from the attribute in the DoD Data Model. To develop generic elements:

- a. First, categorize the data element into a general class (class word).
- b. Second, sub-categorize the data elements within each class based on like metadata attributes.



4. Generic elements, like data elements, are developed and approved in accordance with the "DoD Data Element Standardization Procedures," (reference (f)).

## G. DATA ELEMENTS

1. A data element is a basic unit of information having a meaning and subcategories (data items) of distinct units and value. Through its name and definition, a data element conveys a single informational concept.

2. All attributes of approved data entities in the DoD Data Model will become standard data elements. As new information requirements are identified for approved prime words, additional data elements are developed and submitted for approval via the "Data Element Standardization Procedures," (reference (f)). Such data elements may not have been approved at the time the data entity was approved; therefore, as these new data elements are approved they are reflected in the DoD Data Model as additions to a data entity.

3. All data elements are approved and documented in accordance with the "DoD Data Element Standardization Procedures," (reference (f)).

a. Any person, either within the Department of Defense or representing a DoD organization, may propose a data element for standardization to their FDAAd or CDAAd .

b. The FDAAd or CDAAd conducts a preliminary review of the data element to ensure adherence to mandatory technical and functional requirements. Upon completion of the preliminary review, the FDAAd or CDAAd will submit the data element for informal review to the FDAAd designated as the data steward and to the DoD DAd.

c. The FDAAd, designated as the data steward, with guidance from the DoD DAd, will conduct an informal review upon receipt of the data element. The FDAAd and the DoD DAd will coordinate and perform concurrent functional and technical reviews. The FDAAd will track the status of the data element and keep the submitting FDAAd or CDAAd informed of progress and results. The FDAAd should coordinate with their functional area experts, including FAPMs, OSD PSAs, and FIMs to ensure that they are fully represented. The FDAAd is also encouraged to discuss data elements with functional counterparts within Components, CDADs, the originator, and other FDAAds. Data elements that meet the criteria are submitted by the FDAAd or CDAAd as a candidate or modified standard data element via the DDRS for formal approval.

d. The formal approval process consists of a technical and functional review and final approval. The purpose of the technical review is to ensure that the candidate standard data element conforms to DoD Data Administration policy and does not conflict with existing standard data elements. The purpose of the functional review is to validate the candidate data element metadata attributes to ensure that the data

element is functionally accurate and complete, and can be used throughout the Department of Defense. The final approval consists of technical and functional approvals based upon the technical and functional reviews and, if needed, mediation. The DAPMO technically approves, the FDAd functionally approves, and the DoD DAd mediates.

4. Data elements are derived from data entities and their attributes identified in logical data models. Each data element represents an entity-attribute combination.

5. The data element name is created by combining the data entity name (prime word) with a data entity attribute name, including class word, from the data model.

6. During data element standardization, data elements are further grouped within a class and categorized in a group of generic elements based upon the same structures and related domains. A data element must be associated with an approved generic element.

## APPENDIX F

### DATA SECURITY AND CONTROL

#### A. INTRODUCTION

1. The growing and changing nature of computer-generated and -maintained data is having a major impact in the areas of data security and control in AIS. Ever-increasing amounts of data of greater complexity are being distributed over a wider area at an accelerating rate. To be effective in such an environment, data security and control policies must be implemented in an integrated manner across systems and organizational boundaries. Correspondingly, data administration is challenged to ensure that its area of responsibility is effectively reflected in the development, and implementation, of an integrated data security and control policy. Data administration must ensure that data is accurate and free from contamination or corruption. This task includes data protection, security, integrity (including synchronization), auditability, and enforcement. Data administration must also ensure its perspective is represented in current policy.

2. Compared to previous methods, current technology, specifically in modern DBMSs, improves access to, and control over, data. This increased access broadens the base of potential users, which increases the risk that unauthorized personnel could obtain sensitive or classified information. Both increased security risks, and the resulting increased access restriction controls, make it imperative that data administration and technical development activities take an active role in supporting system security by designing and employing the additional security capabilities offered by the DBMS. Data administration will be directly involved in the planning and analysis of security controls as they relate to data stewardship and integrity.

a. Stewardship of data, and control exerted by the data steward to establish rules for granting privileges to access items of data in the "system" of DoD databases, is one of the major responsibilities of data administration. Data administration must, therefore, work with customers to resolve all issues to provide maximum functionality and data sharing while at the same time preserving confidentiality and quality of the data being managed.

b. In addition to system security, data administration is responsible for the assurance of integrity, and auditability of data in the system. Data integrity requires verifying that data values conform to the set of allowed values designated for their data types and identifying those data values that do not conform. Data integrity includes the discipline of data synchronization (the timing requirements of, or between, data elements). In addition, data integrity also includes accuracy, consistency, reliability, validity, completeness, and relevancy. Even if the data in a "system" of DoD databases is verified to be correct when the data enters a database, it still must be

protected from unauthorized access and alterations while in the database. Providing for auditability makes it possible to determine the effectiveness of the data protection, security, and integrity procedures of the systems.

## B. DATA STABILITY

A critical foundation of an organization's data security and control effort is the stabilization of data both within an organization and across organizational lines. Data stabilization involves the disciplined and precise definition of application- independent data requirements so that the data are subjected to minimal change. When change is required, data stabilization practices hold that the change should be predictable, disrupt the overall data architecture to a minimum degree, and be executed in an auditable manner.

## C. DATA SECURITY

Current data security concerns have evolved from a concern for the procedures that use data to the actual data itself. This has focused attention on the idea that data have become an asset with their own integral value. As the way in which we use data undergoes basic changes, so must the approach to data security. The new environment demands that security, including the protection of data subject to use, release, or disclosure restrictions, be implemented in an integrated fashion. Data administration must be proactive in examining all areas of security, including the protection of data subject to use, release, or disclosure restrictions, to ensure that the data administration perspective is properly represented. As data is distributed on a broader scale, there are attendant issues that can only be addressed by an authority with a global view. Data security is no longer a function that is mandated by higher authority and executed within individual systems.

## D. DATA CONTROL

Although data control is treated as a separate topic from data security, the two are inextricably bound. Data control will be considered from the perspective of its three major components: data integrity, auditability, and enforcement. Data integrity can be considered the requirement; auditability and enforcement as the tools for ensuring compliance with this requirement.

### 1. Data Integrity.

Data integrity seeks to ensure that the DBMS will perform its function consistently. That is, it will preserve data without unintentional change, produce results that are correct to the defined degree of precision, maintain data availability, and, whenever possible, allow only a single point-of-entry for the data, regardless of where and how it is used.

a. Data administration's concern for data integrity requires that data values (at the database level) be verified to conform to the set of allowed values designated for their data type. These permitted values arise from the management requirements of the organization.

b. Management requirements are represented in logical models or specifications that guide the development of the physical system or database that will manage the actual values of data stored in databases. However, data integrity, from design to physical management and maintenance, is a common goal of both the physical and logical efforts.

(1) During the design phase, logical data structures need to be developed that ensure that data values can be verified to conform to the specific values, or set of permitted values, designated for their data types.

(2) Data and database integrity focuses on the usage of data. It incorporates the concept of synchronization. In addition, data integrity also includes validity, completeness, and relevancy. Each of the goals of data integrity are briefly defined in Figure F-1, below.

## 2. Auditability

a. Auditability is the measure of a system's capacity to link defined classes of information across the full breadth of a given environment. From the traditional security perspective, this ability has been most often associated with the management of access control: recording what attempts have been made to access the system and what activities were undertaken upon access being granted. However, as we are increasingly faced with security for distributed systems and inter-organization data, the challenge of auditability has become much broader and more complex.

b. Data administration must establish procedures for auditing individual systems in a manner that balances budget constraints and the reliability of audits. Each system must be mandated to be able to provide a complete description of its metadata in a form defined by the auditing authority and which that authority can automatically process. The system being audited must produce its metadata description in a manner that is as automated as possible so as to ensure that the description is an accurate snapshot of the system as it is currently operating. To ensure data is afforded the appropriate level of security and its integrity is ensured, the data values must be adaptable to their original producer, and metadata must be adaptable to both the source from which it was immediately derived, and also the ultimate authority for that metadata. These audit trails cannot be effectively established unless effective data stability has also been established. The audit trails for metadata and data values should be pursued as two separate, albeit, complementary efforts. To attempt to implement the two concurrently would result in an unnecessarily complex system.

### 3. Enforcement

Data administration must provide primary support for the enforcement of standards. The data administrator must report any non-compliance with standards to the appropriate authority. Data administration should also be prepared to provide sufficient background information on the circumstances of the non-compliance so that an intelligent judgment can be made by responsible authorities. The application, or system, that is responsible for the non-compliance should be specifically identified and also be able to provide background information to the appropriate authority.

1. Consistency. Data is maintained so that it is free from variation or contradiction.
2. Accuracy. Correct data that conforms to models derived to support enterprise requirements and standards, and user requirements.
3. Timeliness. A condition requiring that a data item or multiple items are provided at the time required or specified.
4. Validity. The quality of maintained data that is found on an adequate system of classification (e.g., data model) that is rigorous enough to compel acceptance.
5. Relevancy. The state of maintaining data in a condition that provides the ability to retrieve the specific information needed by the user.
6. Relatability. The quality of data that permits it to be rationally correlated or compared with other similar or like data.
7. Stability. The ability of a data structure to satisfy additional or changing information needs over time without affecting its original design.
8. Extensibility. The ability of a data structure to accommodate additional values or iterations of data over time without impacting its initial design.
9. Flexibility and/or Modularity. The ability of data structure design to accommodate requirements of change in process without data reengineering or at a minimum not affect major components of the design to accommodate such changes.

Figure F-1. Definitions of the goals of data integrity.

## APPENDIX G

### DATABASE ADMINISTRATION CONCEPTS

#### A. INTRODUCTION

1. In general, the role of database administration, like that of data administration, applies to many DoD organizations and projects and requires levels of database administration parallel to those of data administration. The requests for technical support for data access will flow from the application-specific to the enterprise-wide level, and the guidance and support will flow from the enterprise-wide to the application-specific level.

2. Database administration is concerned with the efficient use of the resources that hold and make available the data resources in assigned databases in an organization. Database administration controls and maintains the flow of data into, within, out of, and among various databases. It physically controls how, where, and in what manner, data is stored and maintained within each database.

3. The relationship between the data administration and database administration function is a mutually supportive one with the combined objective of building integrated "systems" of databases capable of sharing data across organizations' functional boundaries. Data administration is a higher level conceptual or architectural discipline that is responsible for data, data structure, and integration of data with activity throughout the data and information systems life-cycle. Database administration, on the other hand, includes the physical design, development, implementation, security, and maintenance of physical databases built to support the logical design developed by the data administration activity. The data administrator provides each database administrator with the boundaries (domains) of a database structure developed from the logical model. While data administration is responsible for interpreting and enforcing information management policies for the enterprise as a whole, database administration is responsible for managing and carrying out those policies for individual databases.

#### B. POLICY

1. Database administration follows the standards and policies established by data administration, bringing problems and necessary changes to the attention of the FDA or CDA, and the AIS PM. Database administration policy also supports the Defense Information Management guiding principles specified in DoD Directive 8000.1 (reference (g)). A summary of the guiding principles that database administration will adhere to is provided below.



- a. Provide the best performance at the least cost for all users while meeting functional and technological requirements.
- b. Data will be controlled and managed throughout its life-cycle as a resource, in the same manner as capital, materiel, and people.
- c. Databases will be designed, implemented, and maintained:
  - (1) Separately from information applications to enable shared and controlled access by multiple users.
  - (2) In an enterprise-wide strategy and in accordance with data life-cycle management practices defined in Appendix A in this Manual.
  - (3) Based on activity and data models that support improved functional practices and value of information.
  - (4) In accordance with DoD Directive 8000.1, (reference (g)) and DoD Directive 8120.1 (reference (b)).
- d. Database products (e.g., schemas) will be maintained to facilitate maximum reuse and shareability throughout the Department of Defense.
- e. Access to data will be facilitated, and/or controlled and limited, as required. Data will also be safeguarded against unintentional or unauthorized alteration, destruction, or disclosure.

### C. DATABASE ADMINISTRATION ACTIVITIES

1. Database administration activities include providing technical support for physical database definition, design, implementation, maintenance, integrity, and security; enforcing the policies and standards established by the data administrator; coordinating with computer operations technicians, system developers, vendors, and users; and education of personnel to ensure competency. The AIS PM has the responsibility for program management and for ensuring that data administration policies and procedures are followed. The database administrator is oriented toward technical support for databases. Appropriate use of information technology resources is a major concern of the database administration activity. The following are major activities of the database administration activity:

- a. Technical Support. The database administrator has the responsibility for the operational implementation of databases, from designing the physical databases and user views to guaranteeing the integrity and efficiency of the data access activities. This is the main activity of the database administrator. The database administrator

shall:

(1) Provide technical advice and guidance for database integration design tools, database access, logical and physical data structure evaluation, and database problem resolution (including recovery and performance issues).

(2) Provide technical assistance in the design of logical data models.

(3) Design and implement optimum physical database structures based on logical data model design and performance requirements. This includes the assessment of future growth via capacity planning.

(4) Promulgate technical standards, design rules, and conventions for databases.

(5) Monitor and maintain technical integrity of physical databases. Establish and promulgate restart and recovery procedures. Conduct continuing technology assessment.

(6) Monitor and analyze database performance on a continuing basis to maintain database efficiency.

(7) Participate in the development of DBMS evaluation criteria and the evaluation and testing of alternate technology solutions.

(8) Provide continuing evaluation and planning to:

(a) Take advantage of evolving technologies.

(b) Support system enhancement and modernization.

(c) Position data for transition (migration, gradual evolution, archival).

b. Enforcement of Policies. This includes security, access, data standardization, and configuration management policies. The database administrator works with the data administrator to provide the degree of protection commensurate with the security classification of the data and the authorization of the user; guarantees compliance with access control standards by establishing and monitoring file protection mechanisms; implements automated support to enforce data standards; and institutes procedures to track and document all changes to database-related items to support configuration management programs. The database administrator shall:

(1) Evaluate and implement database security packages, monitor database security, and provide control and access to databases in accordance with

data stewardship guidelines for database configuration items.

(2) Enforce and execute data standardization and data life-cycle policies established by data administration.

c. Coordination. The database administrator coordinates all database-related issues with data administration, computer operations, technical development activities, and users. This includes implementing and maintaining and/or converting databases, assuring consistency with the logical data model, establishing procedures for the release of database schemas and subschemas to operational sites, and addressing technical questions and resolving technical problems. The AIS PM ensures that the coordination follows data administration policies and procedures.

d. Education. The database administrator establishes procedures that support the implementation, promulgation, and continuity of an effective education program, including formal training. The areas of database concepts, database design, effects of database operation, database standards, database usage, and high-level languages are addressed. The database administrator will also liaise and consult about proper database practices with management, technical development activities, AIS PMs, users, and other involved personnel. The database administrator shall provide training in proper database practices to these people.